УДК 654.924.3

О проведении аудита защищенности организационного канала утечки информации, составляющей коммерческую тайну организации

Тельный А. В., Яковлева Е. И., Романова А. Г.

Постановка задачи. *Современное развитие информационных технологий, средств информатизации и передачи данных, влечет за собой повышение значимости защиты информации, составляющей коммерческую тайну в организации. Утечка информации, являющейся коммерческой тайной в организации происходит в основном по организационному каналу, состояние защиты которого необходимо постоянно контролировать.* ***Целью работы*** *является формирование методики для оценки защищенности организационного канала утечки информации, составляющую коммерческую тайну в организации. Данная методика может быть использована для автоматизации контроля исполнения требований нормативных документов в области информационной безопасности, оценки уровня исполнительской дисциплины сотрудников и проверки знаний и навыков в области информационной безопасности персонала объекта.* ***Используемые методы.*** *Для анализа защищенности организационных каналов утечки информации использованы стандартные методы системного анализа, морфологического анализа, методы экспертных оценок.* ***Новизна.*** *Новизна представленного решения заключается в создании авторами типовых перечней источников и причин утечки информации, организационных и технических защитных механизмов, критериев оценки частных и групповых показателей защищённости организационного канала утечки информации.* ***Результат.*** *Сформирована методика проведения аудита защищенности организационного канала утечки информации, составляющей коммерческую тайну организации.* ***Практическая значимость.*** *Разработанная методика может быть реализованы в виде системы поддержки принятия решений для проведения аудита защищенности организационного канала утечки информации, составляющей коммерческую тайну организации.*

Ключевые слова: *информационная безопасность, разглашение информации, утечка информации по организационному каналу, аудит защищенности организационного канала, коммерческая тайна организации.*

Введение

В настоящее время одной из самых вероятных причин утечки информации в организациях является ее разглашение, что расценивается как утечка по организационному каналу [1], и по оценкам различных источников [2, 3] составляет до 60-70% возможных инцидентов безопасности, связанных с утечкой информации. Для обеспечения защиты информации в организации принимается комплекс мер организационного характера для обеспечения режима ограниченного доступа обращения с защищаемой информацией. Для сведений, отнесенных к государственно тайне это режим секретности, для сведений конфиденци-

Библиографическая ссылка на статью:
Тельный А. В., Яковлева Е. И., Романова А. Г. О проведении аудита защищенности организационного канала утечки информации, составляющей коммерческую тайну организации // Системы управления, связи и безопасности. 2019. № 2. С. 236-277. DOI: 10.24411/2410-9916-2019-10212.

Reference for citation:
Telny A. V., Iakovleva E. I., Romanova A. G. Audit of security of the organizational channel of information leakage which is the trade secret of the organization. *Systems of Control, Communication and Security*, 2019, no. 2, pp. 236-277. DOI: 10.24411/2410-9916-2019-10212 (in Russian).

ального характера, в том числе коммерческой тайны, вводится режим конфиденциальности или режим коммерческой тайны. Однако, наличие нормативной и организационно – распорядительной документации по обеспечению режима секретности или конфиденциальности на объекте защиты еще не определяет высокий уровень защищенности организационного канала утечки информации. Для защиты информации от утечки по организационному каналу необходимо осуществлять постоянный объективный контроль качества исполнения требований нормативных документов и локальных нормативных актов по обеспечению безопасности обращения с информацией ограниченного доступа.

Вопросы защиты секретных сведений от утечки по организационному каналу довольно подробно регламентированы нормативно-распорядительными документами государственных регуляторов, которые являются лицензиарами в области защиты сведений, составляющих государственную тайну. Вопросы защиты сведений, составляющих коммерческую тайну (КТ), определены только в рамках Федерального закона Российской Федерации №98 от 2004 года «О коммерческой тайне». Контроль фактического исполнения организационных мероприятий по защите коммерческой тайны со стороны государства не регулируется. Кроме того, в настоящее время не существует общепринятой методики аудита для анализа защищенности организационного канала утечки информации, составляющей коммерческую тайну в организации.

Организации, в которых введен режим коммерческой тайны, устанавливают и обеспечивают контроль защиты организационного канала утечки информации, руководствуясь только собственными, локальными нормативными актами. Для защиты коммерческой тайны приходится принимать серьезные организационные и технические меры, иногда «по аналогии» с мерами, необходимыми для защиты сведений составляющих государственную тайну. Поэтому задача обеспечения оценки защищенности коммерческой тайны организации от разглашения является весьма актуальной.

По данной тематике имеется ряд монографий и научных статей, в которых исследовались теоретические основы обеспечения защиты информации от ее разглашения. Проблемы организационной и правовой защиты информационных ресурсов рассматривались в научных работах таких авторов как Аверченков В.И., Степанов Е.А., Копылов В.А., Полякова Т.А., Ищейнов В.Я., Скрыль С.В. и других [1, 4, 5].

Вопросам технической защиты организационного канала утечки информации посвящены работы Хорева А.А., Меньшакова Ю.К., Зайцева А.П. и других. Общие подходы к организации защиты конфиденциальной информации в коммерческих структурах изложены в [6, 7, 8].

Теоретические исследования за рубежом имеют значительную специфику в связи с совершенно иным характером национальных законодательств в области коммерческой тайны организаций. Для защиты организационного канала утечки информации представляют интерес исследования в сфере обеспечения физической защиты объектов от несанкционированного доступа, реализации контрольно-пропускного и объектового режима. Данные исследования проводились в национальной лаборатории «Сандия» (США), международной ассоци-

ации частных охранных консультантов и других организациях. Наибольший интерес представляют работы Mary Lynn Garcia, James F. Broderp, Charles A. Sennewald [9, 10] и других.

Как правило, при оценке защищенности организационного канала на предмет возможности утечки информации, составляющей коммерческую тайну, проверяется только выполнение организационно-распорядительных документов по режиму коммерческой тайны и обстоятельства произошедших инцидентов информационной безопасности на предприятии. Принципиальное отличие предлагаемой методики от аналогичных заключается в многофакторном рассмотрении организационных и технических аспектов контроля состояния защиты организационного канала. Информация об организационных и технических показателях защищенности собирается более полно, чем в стандартных методиках, с помощью документальных проверок, опросов, негласных проверок, тренировок и тестов, технических обследований, использования протоколов функционирования технических средств, анализ технических характеристик оборудования и т.д.

Методика аудита защищенности организационного канала утечки информации, составляющей коммерческую тайну организации

Для анализа защищенности организации от утечки информации, составляющей коммерческую тайну, по организационному каналу, предлагается использовать следующую последовательность действий.

1. Определяется группа экспертов, численностью не менее пяти человек, которая используя разновидности методов «мозгового штурма» (метод «мозговой атаки» или свернутой «мозговой атаки»; морфологического анализа; сценариев; суда; синектики; метод Гордона и др.), определяет основные организационные каналы утечки информации, составляющей коммерческую тайну организации. При этом рассматривается максимально возможное количество различных вариантов утечки информации, и формируются групповые показатели оценки защищенности организационного канала утечки информации, составляющей коммерческую тайну организации. Таким образом, при формировании методики всего было получено K_i, i=1…23 показателя, представленные в приложении 1. Фактически каждый показатель соответствует организационному каналу утечки информации или его части.

2. Той же рабочей группой экспертов по каждому из групповых показателей формируются частные показатели оценки защищённости организационного канала, относящиеся к двум типам, организационные и технические показатели. Организационные показатели: документальная проверка (по факту наличия, полноты и степени выполнения организационно-распорядительных и нормативных документов); по опросам (анкетированию или тестированию) сотрудников; по результатам негласных проверок (скрытого наблюдения за действиями сотрудников). Технические показатели: работоспособность технических средств защиты информации (ТСЗИ) от утечки по техническим каналам и ТСЗИ от несанкционированного доступа; достаточность технических средств (определяется при обследовании состояния технических средств); наличие,

полнота и качество проведения технического обслуживания ТСЗИ; сравнительный анализ протоколов программного обеспечения различных ТСЗИ; просмотр средств видеонаблюдения. При классификации частных показателей и отнесения их к групповым показателям экспертной группой используются методы морфологического анализа. Для определения значения некоторых частных показателей (например, достаточность ТСЗИ), могут быть использованы отдельные методики [11, 12]. В результате работы экспертов формируются две таблицы организационных и технических частных показателей оценки защищённости организационного канала, которые приведены в приложении 2 и приложении 3. В данных таблицах нумерация частных показателей оценки защищенности, соответствует номерам групповых показателей.

3. Той же рабочей группой экспертов, но уже индивидуально, для каждого частного организационного и технического показателя уточняется способ (методика) его получения, и качественные градации состояния исполнения (например, да, нет, частично). Далее, методом двухтурового анкетирования определяется общие решения группы экспертов, которые заносятся в таблицы показателей способов получения и градаций состояния исполнения, организационных и технических частных показателей оценки защищённости организационного канала, которые приведены в приложении 4 и приложении 5. Эксперты устанавливают для каждой градации исполнения показателя численный коэффициент M_{ij} – значение степени выполнения требований для частного показателя от 0 (полное неисполнение) до 1 (полное исполнение). Таким образом, устанавливается однозначная связь между качественными и количественными значениями градациями исполнения частного показателя.

4. Той же рабочей группой экспертов, индивидуально, для каждого частного организационного и технического показателя вводятся коэффициенты n_{ij} – значение важности частного показателя; d_{ij} – значение достоверности частного показателя, где i – номер группового показателя; j – номер частного показателя в группе; J – количество частных показателей для данного номера группового показателя. Значение важности частного показателя означает роль, которую играет частный показатель в исполнении группового показателя, его величина оценивается от 0 до 1. Достоверности частного показателя означает величину субъективизма получения значения показателя, и эта величина оценивается также от 0 до 1.

5. Методами экспертных оценок обрабатываются результаты работы группы экспертов и находятся результирующие экспертные оценки $\bar{n}_{ij}$ и $\bar{d}_{ij}$, которые заносятся в таблицы приложения 2 и приложения 3. Пусть в работе участвует Q экспертов. Каждому эксперту назначают свой весовой коэффициент. Например, экспертов ранжируют по профильности образования V_q и опыту (стажу работы) S_q. Параметры ранжирования считают равнозначными, эксперты проводят работу индивидуально и их мнения независимы между собой. Пусть по каждой из градаций весовых коэффициентов экспертов дают от 0 до F

баллов. Тогда результирующие экспертные оценки можно определить следующим образом:

$$\overline{n} = \frac{\sum_{q=1}^{Q} n_n \left(\frac{V_q + S_q}{2F} \right)}{\sum_{q=1}^{Q} \left(\frac{V_q + S_q}{2F} \right)}; \quad \overline{d} = \frac{\sum_{q=1}^{Q} d_p \left(\frac{V_q + S_q}{2F} \right)}{\sum_{q=1}^{Q} \left(\frac{V_q + S_q}{2F} \right)},$$

где n_q и d_q – экспертные оценки q-го эксперта.

6. Далее проводятся вычисления оценки групповых показателей K_i, которые вычисляются из оценок входящих в них частных показателей:

$$K_i = \frac{\sum_{j=1}^{J} \left(M_{ij} \overline{n}_{ij} \overline{d}_{ij} \right)}{\sum_{j=1}^{J} \overline{n}_{ij} \overline{d}_{ij}},$$

где M_{ij} – значение степени выполнения требований для частного показателя, взятое из таблиц приложения 4 и приложения 5.

7. Той же рабочей группой экспертов устанавливаются уровни соответствия значения оценки группового показателя K_i требованиям по недопущению утечки информации по организационному каналу. Далее, методом двухтурового анкетирования определяется общие решения группы экспертов. По предлагаемой авторами методике, если значение группового показателя K_i лежит в интервале от 0 до 0,25, то данному i-му направлению присваивается нулевой уровень соответствия требованиям по недопущению утечки информации по организационному каналу. Соответственно, если значение K_i лежит в интервале от 0,25 до 0,5 – 1 уровень; от 0,5 до 0,7 – 2 уровень; от 0,7 до 0,85 – 3 уровень; от 0,85 до 0,95 – 4 уровень и от 0,95 до 1,0 – 5 уровень соответствия требованиям по недопущению утечки информации по организационному каналу.

7. Для общей оценки защищенности организационного канала вводится интегральный показатель R, при этом оцениваются только групповые показатели. Как правило, при комплексных инспекционных проверках в системе правоохранительных органов, интегральный показатель защищенности оценивается качественно, только как удовлетворительный или не удовлетворительный (соответствует или не соответствует). Для сведений, составляющих коммерческую тайну организации можно принять аналогичный критерий. Общая оценка интегрального показателя R выставляется либо по минимальному уровню (показатель, являющийся «слабым звеном») $R = \min\{K_1; K_2; ....K_I\}$, или по логическим правилам, установленным экспертами, аналогично пунктам 4 и 5. Например,

$$R = \frac{\sum_{i=1}^{I} \left(K_i \left(1 - \overline{P}(K_i) \right) \right)}{\sum_{i=1}^{I} \left(1 - \overline{P}(K_i) \right)},$$

где $\overline{P}(K_i)$ – результирующая оценка экспертами вероятности (от 0 до 1) утечки информации по данному групповому показателю, при формировании предпосылок (шансов) утечки информации. Расчеты для каждого группового показателя значений $\overline{P}(K_i)$ проводятся аналогично пунктам 4 и 5 и представлены в приложении 1.

8. Той же рабочей группой экспертов устанавливается пороговое значение интегрального показателя *R*, при котором качественно оценивается состояние защищенности организационного канала в целом как удовлетворительное или не удовлетворительное. По предлагаемой авторами методике, при $R < 0{,}85$ защищенность организационного канала следует считать не удовлетворительной.

Адаптация методики аудита защищенности организационного канала

В соответствии с видом деятельности организации, ее структурой, степенью конфиденциальности информации, ведомственной принадлежностью, контингентом работников, нормативно-распорядительными документами в данной сфере, разработанными в самой организации и т.д., для практического использования предлагаемой методики предлагается провести ее адаптацию для конкретной организации. Адаптация проводится только один раз при внедрении методики аудита в организации, при этом собирается группа экспертов, численностью не менее пяти человек, которая анализирует существующие базовые таблицы методики, представленные в приложениях.

1. Проводится анализ групповых показателей оценки защищенности организационного канала утечки информации, представленных в приложении 1. В процессе анализа, часть групповых показателей может быть исключена, или некоторые групповые показатели будут разбиты на составные части, или введены новые групповые показатели, не учтенные в методике.

2. Анализируются частные организационные и технические показатели, приведенные в приложении 2 и приложении 3. Если экспертами были исключены некоторые групповые показатели, то из таблиц исключаются и соответствующие им частные организационные и технические показатели. Возможно исключение или введение новых частных организационных и технических показателей по действующим групповым показателям.

3. Той же рабочей группой экспертов для каждого частного организационного и технического показателя уточняется способ его получения, и качественные градации состояния исполнения. Далее, аналогично пункту 3 методики, для каждой градации исполнения показателя, эксперты устанавливают заново или оставляют без изменений численный коэффициент M_{ij} – значение степени выполнения требований частного показателя.

4. Аналогично пунктам 4 и 5 методики экспертами пересматриваются n_{ij} – значение важности частного показателя; d_{ij} – значение достоверности частного показателя, и рассчитываются результирующие экспертные оценки $\overline{n}_{ij}$ и $\overline{d}_{ij}$, которые заносятся в таблицы приложения 4 и приложения 5.

5. Далее, той же рабочей группой экспертов пересматриваются уровни защищенности организационного канала по групповым показателям (пункт 7 методики). Устанавливаются новые логические правила (при необходимости) для оценки интегрального показателя R и устанавливается его пороговое значение, при котором состояние защищенности организационного канала определяется как удовлетворительное или не удовлетворительное.

После проведения адаптации методики, проведение аудита защищенности организационного канала можно осуществлять силами сотрудников организации, в порядке внутреннего контроля.

Проведение аудита защищенности организационного канала

Фактически, аудит защищенности организационного канала заключается в определении M_{ij} результата выполнения требований частных организационных и технических показателей, прописанных в методике. При проведении аудита защищенности организационного канала утечки информации, составляющей коммерческую тайну организации, по адаптированной для этой организации типовой методике, возможны два варианта ее реализации.

Во-первых, можно составить в бумажном виде бланки таблиц проведения аудита, с выставлением оценок M_{ij} проверяющего по частным организационным и техническим показателям. При этом процесс аудита состоит из сбора информации и обработки результатов.

Во-вторых, более перспективным, является автоматизация проведения аудита и создание системы поддержки принятия решений для проверяющего сотрудника.

При этом, в оболочку интерфейса можно интегрировать нормативно-правовую базу организации по обеспечению режима коммерческой тайны и рекомендации или методики по определению значений некоторых частных показателей (например, методики проверки протоколов работы технических средств, работоспособности технических средств, проведения негласных проверок и т.д.). При проведении аудита защищенности организационного канала впервые, групповые показатели и интегральный показатель защищенности будут мало информативны для оценки деятельности лиц, ответственных за конфиденциальность коммерческой тайны в организации.

Для оценки деятельности должностных лиц, ответственных за защиту коммерческую тайны в организации, необходимо контролировать изменение динамики групповых показателей и интегрального показателя защищенности организационного канала за время между проведением проверок. При значении R более заданного порога (например, при $R \geq 0{,}85$) и выполнения условий $\Delta K_i = K_i(t_2) - K_i(t_1) \geq 0 \ \ (t_2 > t_1)$ и $\Delta R = R(t_2) - R(t_1) \geq 0 \ \ (t_2 > t_1)$, деятельность по защите организационного канала от утечки информации можно считать успешной. Здесь $\Delta t = t_2 - t_1$ период между проведением проверок.

Выводы

Предложенная авторами методика оценки защищенности организационного канала утечки информации, составляющей коммерческую тайну организации, может быть программно реализована для автоматизации проведения аудита информационной безопасности. Предлагаемая методика может быть адаптирована с учетом особенностей и специфики организации. Полученные оценки позволяют выявлять организационные «уязвимости» в системе защиты информации, те направления деятельности, по которым состояние защищенности по организационному каналу является не удовлетворительным. Кроме того, автоматизация проведения аудита позволит проводить проверки своим силами без привлечения сторонних специалистов.

При практическом использовании данной методики необходимо отслеживать динамику изменения групповых показателей K_i и интегрального показателя R между временными интервалами проведения аудита защищенности организационного канала. Представленная методика является модифицированным вариантом более ранней работы [13]. Дальнейшее совершенствование представленной методики заключается в формировании градаций значимости допущенных нарушений по частным организационным и техническим показателям. Кроме того, для каждой градации нарушений можно на основании статистических данных [14] или экспертных оценок проводить оценку вероятности утечки информации из-за допущенного нарушения.

Таким образом, зная допущенные нарушения и продолжительность времени их существования, можно будет оценивать вероятность совершения факта утечки конфиденциальной информации, составляющей коммерческую тайну организации.

Приложение 1

Показатели оценки защищенности
организационного канала утечки информации

Таблица П1 – Групповые показатели оценки защищенности
организационного канала утечки информации

Номер показателя	Содержание показателя	$\overline{P}(K_i)$
1	2	3
K_1	Выполнение требований нормативных и организационно-распорядительных документов по организации конфиденциального делопроизводства	0,4
K_2	Выполнение требований нормативных и организационно-распорядительных по защите информации при проведении совместных работ, выполняемых предприятием в его производственной и иной деятельности	0,7
K_3	Выполнение требований нормативных и организационно-распорядительных документов по проведению совещаний (конференций и т.д.) в ходе которых обсуждаются вопросы конфиденциального характера	0,5
K_4	Выполнение требований нормативных и организационно-распорядительных документов по защите информации при осуществлении выезда за границу сотрудников, допущенных к конфиденциальной информации, в т.ч. в служебные командировки	0,3

K_5	Выполнение требований нормативных и организационно-распорядительных документов по защите информации при осуществлении рекламной и издательской (публикационной) деятельности	0,8
K_6	Выполнение требований нормативных и организационно-распорядительных документов по защите информации при осуществлении сотрудничества с иностранными государствами (их представителями и организациями)	0,5
K_7	Выполнение требований нормативных и организационно-распорядительных документов по защите информации при осуществлении научных исследований, научно-исследовательских и опытно-конструкторских работ	0,4
K_8	Выполнение требований нормативных и организационно-распорядительных документов по защите информации при передаче сведений о деятельности предприятия и данных о его сотрудниках в территориальные инспекционные и надзорные органы, органы государственной власти	0,2
K_9	Выполнение требований нормативных и организационно-распорядительных документов при осуществлении установленного порядка контрольно-пропускного режима	0,7
K_{10}	Выполнение требований нормативных и организационно-распорядительных документов при осуществлении установленного порядка объектового режима	0,4
K_{11}	Выполнение требований нормативных и организационно-распорядительных документов при принятии решений о защите объекта от несанкционированного доступа. Недопущение ошибочных технических и организационных решений по размещению технических средств систем контроля и управления доступом (СКУД), позволяющим осуществить несанкционированный доступ (НСД)	0,3
K_{12}	Выполнение требований нормативных и организационно-распорядительных документов при принятии решений о защите объекта от несанкционированного доступа. Недопущение ошибочных технических и организационных решений по размещению технических средств охранно-тревожной сигнализации (ОТС), и инженерно-технического укрепления (ИТУ), позволяющим осуществить НСД	0,3
K_{13}	Выполнение требований нормативных и организационно-распорядительных документов по защите информации в технических средствах передачи информации (ТСПИ). Недопущение ошибочных технических и организационных решений по защите информации в ТСПИ	0,6
K_{14}	Выполнение требований нормативных и организационно-распорядительных документов при использовании технических средств защиты информации от утечки по техническим каналам. Недопущение ошибочных технических и организационных решений по защите информации при использовании технических средств защиты информации от утечки по техническим каналам	0,3
K_{15}	Выполнение требований нормативных и организационно-распорядительных документов по защите информации при уничтожении носителей конфиденциальной информации	0,3
K_{16}	Выполнение требований нормативных и организационно-распорядительных документов по защите информации при утилизации производственного брака	0,6
K_{17}	Выполнение требований нормативных и организационно-распорядительных документов по защите информации при хранении и транспортировке продукции конфиденциального характера	0,6
K_{18}	Выполнение требований нормативных и организационно-распорядительных документов по защите информации при приеме на работу персонала	0,7
K_{19}	Выполнение требований нормативных и организационно-распорядительных документов по защите информации при осуществлении допуска к конфиденциальной информации	0,8
K_{20}	Выполнение требований нормативных и организационно-распорядительных документов по защите информации при контроле недопущения физического и психологического воздействия на персонал предприятия, допущенный к конфиденциальной информации	0,3
K_{21}	Выполнение требований нормативных и организационно-распорядительных документов по обеспечению требований к морально-психологическому климату в коллективе и состоянию сотрудников	0,3
K_{22}	Выполнение требований нормативных и организационно-распорядительных документов по защите информации при обеспечении обучения персонала и сотрудников предприятия обращению с информацией конфиденциального характера и носителями такой информации	0,8

K_{23}	Выполнение требований нормативных и организационно-распорядительных документов по защите информации при обеспечении защиты персональных данных сотрудников, допущенных к конфиденциальной информации	0,2

Приложение 2

Таблица П2 – Организационные частные показатели оценки защищённости организационного канала утечки информации

№ группового показателя	№ частного показателя	Содержание частного показателя	$\overline{n}_{ij}$	$\overline{d}_{ij}$
1	2	3	4	5
1	1.1	Инструкция по организации конфиденциального делопроизводства (ДП)	0,9	1,0
	1.2	Положение о подразделении, осуществляющим конфиденциальное ДП	0,85	1,0
	1.3	Перечень сведений, составляющих коммерческую тайну (КТ);	1,0	1,0
	1.4	Наличие постоянно действующей экспертной комиссии (ПДЭК);	0,95	1,0
	1.5	Режим КТ и положение о разрешительной системе доступа к КТ	1,0	0,95
	1.6	Инвентаризация документов и носителей КТ	1,0	1,0
	1.7	Хранение и обработка документов и носителей КТ в специальных помещениях и выполнение требований к ним	0,9	0,9
	1.8	Инструкция по использованию электронной подписи (ЭП) и специального ПО в системе электронного документооборота (СЭД) (при наличии)	0,8	1,0
	1.9	Должностные обязанности лиц, занимающихся конфиденциальным ДП	0,8	1,0
	1.10	Документальное сопровождение работы с КТ, в т.ч. ведение соответствующих журналов (по внутренним распорядительным документам) приема-сдачи помещений с КТ под охрану (или протоколы АРМ), выдачи ключей, выдачи носителей с КТ (карточки-заместители) и т.д.	0,8	0,75
	1.11	Аудит информационной безопасности в СЭД, использование глобальных и беспроводных сетей, СЗИ, антивирусного ПО, сетевых экранов и т.д.	0,8	0,85
	1.12	Использование сертифицированного ПО, аттестация, категорирование объектов информатизации (ОИ) (при необходимости и т.д.).	0,9	1,0
2	2.1	Договор о проведении совместных работ, раздел по обеспечению конфиденциальности	1,0	1,0
	2.2	Инструкции по контрольно-пропускному и объектовому режиму (КПиОР), организация доступа только лиц, определенных договором и допуск к КТ-наличие соответствующих распоряжений	0,9	1,0
	2.3	Инструкции по КПиОР в части ограничения передвижения сторонних сотрудников по предприятию	0,9	1,0
	2.4	Инструкции по КПиОР в части закрепления сопровождающих (ответственных за сопровождение) сотрудников предприятия	0,9	1,0
	2.5	Проведение мероприятий по недопущению неформального общения лиц, допущенных к КТ разных организаций	0,8	0,6
	2.6	Контроль лиц, находящихся в служебных командировках в служебное и не служебное время	0,7	0,4
	2.7	Использование специальной или фельдъегерской связи (при необходимости)	1,0	0,7
3	3.1	План проведения совещаний (конференций, симпозиумов и т.д.)	1,0	1,0
	3.2	Организация встречи, размещения и сопровождение приглашенных лиц по территории организации	0,8	0,75
	3.3	Мероприятия по досмотру (при необходимости) участников совещания и организация хранения личных вещей участников совещания	0,9	0,75
	3.4	Инструктажи по обеспечению защиты КИ участников совещания	0,8	0,75
	3.5	Организация максимального удаления из помещения при проведения совещания ОТСС и ВТСС (по возможности)	0,85	0,9
	3.6	Ограничение доступа приглашенных лиц по территории предприятия и в помещения проведения совещания	0,9	0,9

	3.7	Контроль рассматриваемых (строго по регламенту плана совещания) вопросов по ходу совещания	0,85	0,8
	3.8	Проведение мероприятий по недопущению неформального общения лиц, допущенных на совещание	0,8	0,75
3	3.9	Проведение мероприятий по недопущению обсуждения КТ в неустановленных помещениях	0,75	0,75
	3.10	Организационные мероприятия по проведению обследований и проверок на предмет выявления средств несанкционированного съема информации («зачистке») помещений до и после совещаний	0,9	0,6
	3.11	Контроль (визуальный) и принятие мер при несанкционированном использовании участниками совещания технических средств	1,0	0,6
	3.12	Обеспечение участников совещания раздаточным материалом	0,85	0,9
	3.13	Обеспечение санкционированной рассылки материалов совещания участникам совещания	0,9	0,9
	3.14	Использование сертифицированных ТСЗИ, при проведении совещаний	0,95	1,0
4	4.1	Действие разрешительной системы выезда в соответствии с существующими распорядительными документами и полное информирование руководства и ответственных лиц о целях и задачах выезда	1,0	1,0
	4.2	Наличие обязательств сотрудника о неразглашении	1,0	0,95
	4.3	Инструктажи сотрудников по обеспечению защиты КТ перед выездом	0,9	0,74
	4.4	Проведение мероприятий по недопущению неформального общения командированных лиц в служебных командировках	0,85	0,6
	4.5	Мероприятия по отслеживанию контактов (по возможности и необходимости) сотрудников за границей	0,8	0,5
	4.6	Обеспечение сопровождения (по возможности и необходимости) делегации или индивидуально (возможен не гласный контроль)	0,8	0,6
	4.7	Досмотр (по возможности и необходимости) багажа и личных вещей сотрудников до и после приезда	0,6	0,6
	4.8	Контроль лиц, находящихся в служебных командировках в служебное и не служебное время	0,7	0,7
	4.9	Отчет по выезду (если он служебный) и подтверждающих документов (командировка, путевка, билеты, визы, отметки в паспортах и т.д.)	0,8	0,95
5	5.1	Наличие ПДЭК и ее фактическая работа по контроля исходящей информации при публикационной деятельности	1,0	0,75
	5.2	Инструктажи сотрудников и ознакомление их с нормативно-распорядительной документацией в данной области	0,95	0,6
	5.3	Взаимодействие со СМИ и планы мероприятий по взаимодействию	0,9	0,75
	5.4	Должностные инструкции ответственных за данное направление работы лиц	0,9	0,7
	5.5	Анализ публикаций, рекламных материалов и др. исходящих документов со стороны ответственных лиц и службы безопасности	0,85	0,75
	5.6	Взаимодействие с другими предприятиями и организациями по вопросам открытого опубликования материалов, содержащих КТ о проводимых совместных и других работах	0,8	0,8
	5.7	Режим КТ и Положение о разрешительной системе доступа к КТ	1,0	0,9
	5.8	Ограничение доступа к КТ лиц, ответственных за взаимодействие со СМИ и рекламу на предприятии	1,0	0,9
	5.9	Недопущение в специальные помещения с КТ экскурсий, журналистов и др.	1,0	0,95
6	6.1	Наличие нормативных документы в данной области и их исполнение	0,85	0,85
	6.2	Утвержденный перечень сведений, контроль передаваемой информации строго по перечню разрешенных к передаче и только в рамках договора	0,9	1,0
	6.3	Наличие разрешительных федеральных нормативных межгосударственных документов (при необходимости)	1,0	1,0
	6.4	Договор о проведении совместных работ с иностранными партнерами, назначение ответственных лиц за информационный обмен	0,9	1,0
	6.5	Инструкция о КПиОР, ограничение передвижения иностранных сотрудников по предприятию	0,9	1,0
	6.6	Инструктажи сотрудников	0,7	0,8
	6.7	Расписки сотрудников о неразглашении	1,0	1,0
	6.8	Проведение мероприятий по недопущению неформального общения с иностранными представителями	0,6	0,7

	6.9	Мероприятия по отслеживанию контактов (по возможности и необходимости) сотрудников предприятия и иностранных представителей	0,8	0,7
	6.10	Наличие ПДЭК и ее работа по контролю передаваемых данных	0,9	0,9
	6.11	Использование специальной или фельдъегерской связи (при необходимости)	0,9	1,0
7	7.1	Наличие нормативных документы в данной области и их исполнение	0,85	0,85
7	7.2	Использование сертифицированного ПО (аттестация и категорирование ОИ при необходимости и т.д.)	0,75	1,0
	7.3	Инструкция по обеспечению КТ при проведении НИР и ОКР	0,85	1,0
	7.4	Наличие ПДЭК и ее работа по контролю исходящей документации по НИР и ОКР	0,9	1,0
	7.5	Контроль ведения патентной документации и лицензионных договоров, юридическое сопровождение данной работы в режиме конфиденциальности	0,9	1,0
	7.6	Осуществление разделения сфер разработки между сотрудниками и отделами (полная информация о разработке должна быть только у ограниченного количества руководителей)	0,7	0,7
	7.7	Инструкция о КПиОР, допуск в определенные помещения только лиц, допущенных к НИР и ОКР (база данных СКУД)	0,8	0,9
	7.8	Хранение и обработка документов и носителей КТ по НИР и ОКР в специальных помещениях и выполнение требований по данным помещениям	0,9	0,9
	7.9	Недопущение передачи информации по НИР и ОКР по открытым каналам связи и телекоммуникаций за пределами режимных помещений	0,9	0,9
	7.10	Использование ТСЗИ от утечки по техническим каналам (при необходимости) при проведении НИР и ОКР	0,95	0,9
	7.11	Периодическая (плановая) и внеплановая инвентаризация информационных документов и изделий (образцов, черновиков, брака и т.д.) содержащих КТ по НИР и ОКР	0,9	1,0
	7.12	Обеспечение требуемого уничтожения и утилизации черновиков, брака и отходов производства	0,8	0,8
	7.13	Контроль по протоколам АРМ СКУД и ОТС посещений помещений, сдаче под охрану помещений уполномоченными лицами	0,8	1,0
	7.14	Документальное сопровождение работы с КТ по НИР и ОКР, в т.ч. ведение соответствующих журналов (по внутренним распорядительным документам) выдачи ключей, выдачи носителей с КТ (карточки-заместители) и т.д.	0,8	0,95
	7.15	Аудит информационной безопасности ОИ, отключение от глобальных и беспроводных сетей, использование антивирусного ПО, сетевых экранов и т.д.;	0,8	0,8
	7.16	Использование специальной или фельдъегерской связи (при необходимости)	0,9	1,0
8	8.1	Инструкция о КПиОР, доступ на территорию и в определенные помещения сотрудников территориальных инспекторских и надзорных органов только с сопровождающими лицами	0,8	1,0
	8.2	Инструктажи сотрудников о порядке допуска и ознакомления с документацией представителей инспекторских и надзорных органов	0,75	0,8
	8.3	Обеспечение передачи материалов только при условиях: на законных основаниях; только с разрешения руководства; только в необходимых объемах; только уполномоченным лицам под расписку	0,9	0,9
	8.4	Обеспечение защиты электронных каналов передачи информации	0,9	0,95
	8.5	Обеспечение защиты персональных данных	0,75	0,9
	8.6	Перечень сведений, составляющих КТ	1,0	1,0
	8.7	Режим КТ и Положение о разрешительной системе доступа к КТ	1,0	1,0
	8.8	Контроль по протоколам АРМ СКУД и просмотр записей системы видеонаблюдения (СВН) посещений помещений предприятия сотрудниками территориальных инспекторских и надзорных органов	0,75	1,0
	8.9	Использование специальной или фельдъегерской связи (при необходимости)	0,9	1,0
9	9.1	Инструкции по КПиОР, организация доступа только лиц, определенных договором и допуск к КТ-наличие соответствующих распоряжений	0,9	1,0
	9.2	Договор и его исполнение с частной охранной организацией (ЧАО) или гос.службой (например, с вневедомственной охраной) по охране объекта и осуществлении КПиОР	0,9	1,0
	9.3	Должностные инструкции сотрудников охраны	0,8	1,0
	9.4	Инструкции о сдаче помещений под охрану, хранении ключей и т.д. (обучение им персонала объекта)	0,95	1,0

	9.5	Ведение исполнительской документации (журналов или протоколов АРМ) при осуществлении КПиОР	0,95	0,85
	9.6	Наличие с службе безопасности (СБ) специалистов в данной области	0,85	1,0
	9.7	Сертификация оборудования и технических средств обеспечения КПиОР	0,8	1,0
9	9.8	Лицензия (и опыт работы) организации, осуществляющей монтаж оборудования для обеспечения КПиОР	0,95	0,95
	9.9	Технический надзор за монтажными и пуско-наладочными работами (со стороны охранной организации)	0,6	1,0
	9.10	Наличие договора и технического обслуживания при эксплуатации технических средств КПиОР (СВН, ОТС, СКУД и др)	0,8	1,0
	9.11	Контроль по протоколам АРМ СКУД и ОТС посещений помещений, сдаче под охрану помещений со стороны СБ предприятия	0,75	1,0
	9.12	Плановые и внеплановые проверки со стороны СБ предприятия физической охраны (соблюдение дислокации, экипировки, действий при реагировании на тревожные ситуации), проведение тренировок и учений физической охраны	0,8	0,85
10	10.1	Инструкции по КПиОР, организация доступа только лиц, определенных договором и допуск к КТ-наличие соответствующих распоряжений	0,9	1,0
	10.2	Договор и его исполнение с ЧАО или гос.службой (например, с вневедомственной охраной) по охране объекта и осуществлении КПтОР	1,0	1,0
	10.3	Должностные инструкции сотрудников охраны	0,9	1,0
	10.4	Наличие с СБ специалистов в данной области	0,85	1,0
	10.5	Обеспечение защиты персональных данных посетителей	0,8	0,8
	10.6	Инструкции о сдаче помещений под охрану, хранении ключей и т.д. (обучение им персонала объекта)	0,9	1,0
	10.7	Ведение исполнительской документации (протоколов АРМ) при осуществлении КПиОР	0,9	0,8
	10.8	Сертификация оборудования и технических средств обеспечения КПиОР	1,0	1,0
	10.9	Лицензия (и опыт работы) организации, осуществляющей монтаж оборудования КПиОР	0,95	0,9
	10.10	Технический надзор за монтажными и пуско-наладочными работами (со стороны охранной организации)	0,7	1,0
	10.11	Наличие договора и технического обслуживания при эксплуатации технических средств КПиОР (СВН, ОТС, СКУД и др.)	0,8	1,0
	10.12	Контроль по протоколам АРМ СКУД и ОТС посещений помещений, сдаче под охрану помещений со стороны СБ предприятия	0,75	0,95
	10.13	Плановые и внеплановые проверки со стороны СБ предприятия физической охраны (соблюдение дислокации, экипировки, действий при реагировании на тревожные ситуации), проведение тренировок и учений физической охраны	0,8	0,8
11	11.1	Договор на монтаж СКУД с организацией, имеющей соответствующую лицензию (членство в СРО) и опыт деятельности	0,85	1,0
	11.2	Технический надзор (чаще всего со стороны охранной организации) и соответствующая проектно-сметная документация;	0,6	1,0
	11.3	Договор и его исполнение с ЧАО или гос.службой (например, с вневедомственной охраной) по охране объекта и осуществлении КПиОР	0,95	1,0
	11.4	Наличие договора и технического обслуживания при эксплуатации технических средств СКУД	0,8	1,0
	11.5	Проведение периодического обследования состояния технических средств СКУД, устранение выявленных ранее недостатков	0,8	0,8
	11.6	Выявление по результатам обследований СКУД ошибок монтажа, программирования и уязвимых мест проходов в СКУД	0,75	0,8
	11.7	Своевременная смена пропусков, идентификаторов, паролей и своевременная ротации информации базы данных СКУД	0,9	0,8
	11.8	Инструкции по использованию СКУД, назначение ответственных за эксплуатацию СКУД и ведение базы данных СКУД	0,8	1,0
	11.9	Должностные обязанности сотрудников, эксплуатирующих СКУД	0,8	1,0
	11.10	Плановые и внеплановые проверки физической охраны предприятия (соблюдение дислокации, экипировки, действий при реагировании на тревожные ситуации, в т.ч. по СКУД), проведение тренировок и учений физической охраны.	0,7	0,7
	11.11	Контроль функционирования СКУД по протоколам работы АРМ СКУД со стороны СБ предприятия	0,6	0,95

12	12.1	Договор на монтаж охранно-тревожной сигнализации (ОТС) с организацией, имеющей соответствующую лицензию (членство в СРО) и опыт деятельности	0,85	1,0
	12.2	Технический надзор (чаще всего со стороны охранной организации) и соответствующая проектно-сметная документация	0,6	1,0
12	12.3	Договор и его исполнение с ЧАО или гос.службой (например, с вневедомственной охраной) по охране объекта	0,9	1,0
	12.4	Наличие договора и технического обслуживания при эксплуатации технических средств ОТС	0,7	1,0
	12.5	Проведение периодического обследования состояния технических средств ОТС, устранение выявленных ранее недостатков	0,75	0,75
	12.6	Выявление по результатам обследований ОТС ошибок монтажа, программирования, уязвимых мест и недоблокировок	0,8	0,7
	12.7	Своевременная ротации информации в базах данных ОТС	0,9	0,85
	12.8	Инструкции по использованию ОТС, назначение ответственных за эксплуатацию ОТС и ведение базы данных	0,85	1,0
	12.9	Должностные обязанности сотрудников, эксплуатирующих ОТС	0,9	1,0
	12.10	Плановые и внеплановые проверки физической охраны предприятия (соблюдение дислокации, экипировки, действий при реагировании на тревожные ситуации, в т.ч. по ОТС), проведение тренировок и учений физической охраны.	0,75	0,7
	12.11	Контроль функционирования ОТС по протоколам АРМ ОТС СБ предприятия	0,8	0,9
13	13.1	Определение перечня и видов защищаемых каналов и средств защиты каналов передачи данных и систем передачи информации (СПИ);	1,0	1,0
	13.2	Положения об отделе и инструкции ТЗИ, исполнение требований данных документов по закрытию каналов передачи данных и СПИ	0,9	1,0
	13.3	Наличие ПДЭК (при необходимости) и ее фактическая работа по контролю закрытия каналов передачи данных и СПИ	0,8	0,7
	13.4	Договор на монтаж технических средств с организацией, имеющей соответствующую лицензию и опыт деятельности	0,9	0,95
	13.5	Наличие с СБ специалистов в данной области	0,8	1,0
	13.6	Использование сертифицированных ПО и технических средств	1,0	1,0
	13.7	Договор с удостоверяющим центром (УЦ) при использовании ЭП (наличие своих УЦ), инструкции сотрудникам	1,0	1,0
	13.8	Аудит информационной безопасности, использование глобальных и беспроводных сетей, ТЗИ, антивирусного ПО, сетевых экранов и т.д.	0,8	0,9
	13.9	Должностные инструкции лиц по данному направлению и обучение персонала закрытию каналов	0,8	1,0
	13.10	Аутентификация и идентификация, контроль по протоколам работы закрытия информации в каналах связи	1,0	0,95
	13.11	Использование средств криптозащиты (при необходимости), их сертификация	1,0	1,0
14	14.1	Проведение специсследований, спецпроверок, спецобследований, категорирование и аттестация объектов информатизации и выделенных помещений (по необходимости требований), должная документация по ним с организации, имеющей соответствующие лицензии	1,0	1,0
	14.2	Проверка эффективности использования ТСЗИ (по требованию нормативных документов)	0,9	0,8
	14.3	Договор на монтаж ТСЗИ с организацией, имеющей соответствующую лицензию и опыт деятельности	0,9	1,0
	14.4	Наличие с СБ специалистов в данной области	0,85	1,0
	14.5	Использование сертифицированных ТСЗИ и ПО	1,0	1,0
	14.6	Аудит информационной безопасности, использование глобальных и беспроводных сетей, ТЗИ, антивирусного ПО, сетевых экранов и т.д.	0,9	0,8
	14.7	Инструкции по эксплуатации ТСЗИ и методики поиска закладных устройств (при необходимости)	0,8	1,0
	14.8	Должностные инструкции лиц по данному направлению и обучение персонала по защите от утечки информации по техническим каналам	0,8	1,0
	14.9	Аутентификация и идентификация, контроль по протоколам работы закрытия информации в технических каналах	0,9	0,8
	14.10	Наличие, функции и ведение документации комиссиями по режиму КТ (конфиденциальности), категорированию объектов информатизации, ПДЭК (при необходимости);	0,8	0,75

	14.11	Положения об отделе и инструкции по ТЗИ, исполнение требований нормативных документов по закрытию информации от утечки по техническим каналам	0,8	0,8
	14.12	Ведение необходимой исполнительской документации использования ТСЗИ (журналы, формуляры и т.д.)	0,75	0,75
14	14.13	Организация обслуживания и поверки ТСЗИ	0,8	0,8
15	15.1	Инструкция по организации конфиденциального ДП	0,9	1,0
	15.2	Инструкция об обеспечении конфиденциальности и режима КТ	0,95	1,0
	15.3	Перечень сведений, составляющих КТ	1,0	1,0
	15.4	Наличие постоянно действующей экспертной комиссии (ПДЭК)	0,9	1,0
	15.5	Режим КТ и Положение о разрешительной системе доступа к КТ	0,9	1,0
	15.6	Инвентаризация документов и носителей КТ	0,9	1,0
	15.7	Хранение и обработка документов и носителей КТ в специальных помещениях и выполнение требований к ним	0,95	0,9
	15.8	Должностные обязанности лиц, занимающихся защитой КТ и конфид. ДП	0,85	1,0
	15.9	Документы (акты) уничтожения и утилизации носителей КТ	0,8	1,0
	15.10	Контроль уничтожения черновиков, образцов, использованных носителей и комиссионная оценка качества утилизации	0,85	0,85
16	16.1	Инструкция об обеспечении конфиденциальности и режима КТ	1,0	1,0
	16.2	Документы (акты) уничтожения и утилизации носителей КТ и производственного брака	0,9	1,0
	16.3	Должностные обязанности лиц, занимающихся утилизацией брака	0,8	1,0
	16.4	Контроль уничтожения черновиков, образцов, использованных носителей и комиссионная оценка качества утилизации	0,9	0,9
	16.5	Наличие договоров со сторонними организациями по утилизации брака (при отсутствии собственных возможностей)	0,75	1,0
17	17.1	Наличие и исполнение инструкции по транспортировке и хранению продукции конфиденциального характера	0,9	1,0
	17.2	Должностные обязанности лиц, занимающихся данными вопросами	0,8	1,0
	17.3	Положения об отделе и инструкции по ТЗИ, исполнение требований данных документов по недопущению утечки информации при хранении и транспортировании продукции конфиденциального характера	0,75	1,0
	17.4	Положения инструкции по КПиОР в данной области	0,8	1,0
17	17.5	Наличие требований (и их соблюдение) по таре, маскировке, маркировке и т.д.	0,8	0,9
	17.6	Наличие системы постоянного контроля сохранности и инвентаризации получения и отгрузки продукции конфиденциального характера	0,8	0,8
18	18.1	Инструкции федеральных ведомственных и др. вышестоящих организаций по приему на работу персонала и соблюдение этих требований в организации	1,0	1,0
	18.2	Внутренние организационно-распорядительные требования в организации по приему на работу персонала и их выполнение	1,0	0,8
	18.3	Инструкция об обеспечении конфиденциальности и режима КТ	1,0	1,0
	18.4	Перечень сведений, составляющих КТ	1,0	1,0
	18.5	Режим КТ и Положение о разрешительной системе доступа к КТ	1,0	1,0
	18.6	Должностные обязанности по должностям кандидатов на работу	0,8	1,0
	18.7	Наличие расписок сотрудников о неразглашении КТ	0,8	1,0
	18.8	Утвержденная номенклатура допущенных к КТ должностей	0,75	1,0
	18.9	Личные дела сотрудников, допущенных к КТ и актуальность их ведения и обновления информации	0,75	0,9
	18.10	Материалы анкет, опросов, обследований и т.д. сотрудников, допущенных к КТ	0,7	0,8
	18.11	Соответствие квалификационных требований сотрудников, допущенных к КТ	0,8	0,9
	18.12	Соответствие требований по сохранности персональных данных сотрудников, допущенных к КТ	0,7	0,9
	18.13	Инвентаризация личных дел сотрудников, допущенных к КТ	0,8	0,9
	18.14	Работа аттестационных и кадровых комиссий в организации	0,8	0,8
19	19.1	Инструкции федеральных ведомственных и др. вышестоящих организаций по организации допуска персонала к КТ и соблюдение этих требований в организации	1,0	1,0
	19.2	Внутренние организационно-распорядительные требования в организации по допуску персонала к КТ и их выполнение	1,0	1,0
	19.3	Инструкция об обеспечении конфиденциальности и режима КТ	1,0	1,0
	19.4	Перечень сведений, составляющих КТ	1,0	1,0
	19.5	Режим КТ и Положение о разрешительной системе доступа к КТ	1,0	1,0

	19.6	Должностные обязанности по должностям, допущенным к КИ	0,8	1,0
	19.7	Наличие расписок сотрудников о неразглашении КТ	1,0	1,0
	19.8	Утвержденная номенклатура допущенных к КИ должностей	0,7	1,0
	19.9	Инструкция по организации конфиденциального ДП	0,8	1,0
19	19.10	Положение о подразделении, осуществляющим конфиденциальное ДП	0,7	1,0
	19.11	Инвентаризация личных дел сотрудников, допущенных к КТ	0,7	0,9
	19.12	Работа аттестационных и кадровых комиссий в организации	0,75	0,8
20	20.1	Инструкции (положения устава и подразделений СБ) по данным вопросам	0,8	1,0
	20.2	Должностные инструкции лиц, ответственных за данное направление	0,9	1,0
	20.3	Организация физической охраны и физического сопровождения лиц (при необходимости), в том числе руководства, кассиров, инкассаторов и т.д.	0,7	0,7
	20.4	Организация индивидуально-воспитательной работы (ИВР) предприятия	0,7	0,5
	20.5	Защита персональных данных сотрудников, допущенных к КТ	0,75	0,6
	20.6	Взаимодействие с правоохранительными органами и частными детективами	0,7	0,5
	20.7	Обеспечение правовой защиты и социальных гарантий сотрудникам	0,75	0,6
	20.8	Страхование сотрудников, допущенных к КТ	0,6	1,0
	20.9	Обеспечение психологической службы и постоянного контроля психического состояния сотрудников, допущенных к КТ	0,7	0,6
	20.10	Обеспечение ежегодной диспансеризации сотрудников, допущенных к КТ	0,6	1,0
	20.11	Работа общественных формирований (совет коллектива, суд чести и т.д.)	0,6	0,8
21	21.1	Отсутствие общественных формирований (если они требуются)	0,7	1,0
	21.2	Отсутствие или недостатки в документации общественных формирований	0,6	0,7
	21.3	Отсутствие ИВР с персоналом или недостатки в документации по ИВР	0,6	0,7
	21.4	Отсутствие или недостатки культурно-просветительской работы в коллективе	0,6	0,6
	21.5	Отсутствие или недостатки спортивно-массовой работы в коллективе	0,6	0,6
	21.6	Отсутствие или недостатки дополнительного морального, материального и трудового стимулирования сотрудников, допущенных к КТ	0,7	0,8
	21.7	Отсутствие или недостатки дополнительной социальной защиты сотрудников, допущенных к КТ	0,8	0,7
	21.8	Отсутствие или недостатки аналитических материалов анализа морально-психологического климата (МПК) коллектива	0,6	0,7
22	22.1	Отсутствие или недостатки в документации по обучению сотрудников (учебные и календарные планы, журналы проведения занятия, конспекты, отсутствие контроля знаний и посещаемости и т.д.);	0,8	0,8
	22.2	Не использование предусмотренных и новых форм и методов обучения	0,7	0,75
	22.3	Не удовлетворительные знания сотрудников (по результатам проверок)	0,9	0,7
	22.4	Результаты служебных проверок по фактам инцидентов с КТ и носителями КТ	0,9	0,7
	22.5	Не проведение дополнительных занятий	0,7	0,8
23	23.1	Соответствие целей и объемов сборов информации ПДн сотрудников, допущенных к КТ	1,0	1,0
	23.2	Отсутствие или недостатки в документации по ПДн сотрудников, допущенных к КТ (по той документации, которая обязательно должна вестись)	0,8	0,75
	23.3	Отсутствие или недостатки в документации по использованию ТС защиты ПДн сотрудников, допущенных к КТ	0,7	0,75
	23.4	Результаты служебных проверок по фактам разглашения ПДн сотрудников	0,7	0,7

Приложение 3

Таблица П3 – Технические частные показатели оценки защищённости организационного канала утечки информации

№ группового показателя	№ частного показателя	Содержание частного показателя	$\overline{n}_{ij}$	$\overline{d}_{ij}$
1	2	3	4	5
1	1.1	Аутентификация и идентификация в СЗЭД (система защищенного электронного документооборота), контроль по протоколам работы в СЗЭД	1,0	1,0

	1.2	Функционирование электронной подписи (при необходимости)	1,0	1,0
	1.3	Автоматизация контроля исполнения и движения документов (как функция СЗЭД)	0,7	1,0
1	1.4	Наличие и работоспособность ТСО, СКУД в помещениях с обработкой и хранением носителей КТ	0,9	0,75
	1.5	Контроль по протоколам АРМ по сдаче под охрану помещений, посещения помещений уполномоченными лицами (СКУД)	0,7	1,0
2	2.1	Контроль перемещения сторонних сотрудников по протоколам СКУД	0,7	1,0
	2.2	Контроль лиц, находящихся в служебных командировках в служебное и не служебное время по каналам связи	0,7	0,6
	2.3	Контроль лиц, находящихся на территории предприятия посредством СВН	0,8	0,6
3	3.1	Использование поисковых технических средств при «зачистке» помещений	0,8	0,6
	3.2	Использование технических средств (ТС) обнаружения диктофонов, мобильных телефонов, видеокамер и т.д.	0,9	0,65
	3.3	Использование ТСЗИ при проведении совещаний	0,95	0,9
	3.4	Использование средств маскировки и пассивной технических средств защиты информации	0,9	0,8
	3.5	Санкционированное использование звукоусилительной аппаратуры и др. технических средств обеспечения проведения совещания	1,0	1,0
	3.6	Использование СКУД при организации доступа на территорию объекта в помещения совещаний	1,0	0,8
	3.7	Использование СВН для контроля перемещения участников совещания	0,8	0,7
4	4.1	Использование технических средств при «зачистке» багажа и личных вещей до и после приезда (при возможности и необходимости)	1,0	0,7
	4.2	Контроль лиц, находящихся в служебных командировках в служебное и не служебное время по каналам связи	0,7	0,6
	4.3	Контроль лиц, находящихся в служебных командировках в служебное и не служебное время по их местоположению (GPS и т.д.)	0,7	0,5
	4.4	Использование полиграфа (по возможности и необходимости)	0,9	0,8
4	4.5	Использование (гласное и негласное, по возможности и необходимости) средств видеофиксации при сопровождении	0,9	0,95
5	5.1	Аутентификация и идентификация в корпоративной вычислительной сети	1,0	1,0
	5.2	Функционирование ЭЦП (при необходимости)	1,0	1,0
	5.3	Аудит информационной безопасности, использование глобальных и беспроводных сетей, ТЗИ, антивирусного ПО, сетевых экранов и т.д.	0,9	0,8
	5.4	Наличие и работоспособность ТСО, СКУД в помещениях с обработкой и хранением носителей КТ	0,9	0,9
	5.5	Использование специализированного ПО анализа информации (по тематике близкой к КТ предприятия) из существующих открытых источников	0,7	0,6
6	6.1	Контроль нахождения иностранных представителей на территории предприятия с помощью СКУД и СВН	0,7	0,9
	6.2	Аутентификация и идентификация в КВС (корпоративной вычислительной сети)	1,0	1,0
	6.3	Технические ограничения и контроль по протоколам (по сотрудникам) контактов с иностранными партнерами по телефонной связи, электронной почте, сетям телекоммуникаций	0,7	0,6
	6.4	Исключение возможности электронных контактов с зарубежными партнерами с СВТ на территории предприятия	0,9	0,6
	6.5	Использование средств ЭЦП и шифрования (при необходимости) при электронном общении с иностранными партнерами	1,0	1,0
7	7.1	Оборудование помещений с проведением работ по НИР и ОКР техническими средствами ОТС, СКУД, СВН и обеспечение их работоспособности	0,95	0,9
	7.2	Использование противокражных систем (например, радиометок) для контроля и учета перемещения между помещениями и выноса из помещений образцов, носителей КТ и т.д.	0,7	1,0
8	8.1	Функционирование средств ОТС, СКУД, СВН и обеспечение их работоспособности	0,95	0,95
	8.2	Использование ЭЦП и средств шифрования (сертифицированного ПО) для закрытия каналов электронной связи с инспекторскими и надзорными органами	1,0	1,0
9	9.1	Функционирование технических средств КПРиОР (ОТС, СКУД, СВН и т.д.) и обеспечение их работоспособности	1,0	0,9

	9.2	Соответствие требованиям нормативных документов по классам защиты технического укрепления элементов строительных конструкций зданий, сооружений, помещений, ограждений территорий, КПП и т.д.	1,0	0,9
10	10.1	Функционирование технических средств КПиОР (ОТС, СКУД, СВН и т.д.) и обеспечение их работоспособности	1,0	0,9
	10.2	Соответствие требованиям нормативных документов по классам защиты технического укрепления элементов строительных конструкций зданий, сооружений, помещений	1,0	0,9
11	11.1	Функционирование технических средств СКУД, обеспечение их работоспособности, полнота и актуальность базы данных	1,0	0,9
12	12.1	Функционирование технических средств ОТС, обеспечение их работоспособности, полнота и актуальность базы данных	1,0	0,9
13	13.1	Контроль протоколов передачи данных по закрытым каналам на предмет выявления несанкционированных действий	1,0	0,8
	13.2	Контроль протоколов на предмет возможности и выявления НСД к информационным ресурсам закрытых каналов	1,0	0,95
	13.3	Контроль ведения установленных журналов информационного обмена (при наличии требований)	1,0	0,95
14	14.1	Контроль протоколов функционирования ТСЗИ	1,0	1,0
	14.2	Обеспечение работоспособности ТСЗИ	1,0	1,0
	14.3	Использование специальных технических средств поиска и обнаружения закладных устройств.	0,8	0,7
15	15.1	Наличие технических средств (способов) уничтожения носителей КТ, образцов, черновиков и т.д.;	1,0	0,8
	15.2	Наличие технических возможностей должной утилизации носителей КТ	1,0	0,9
16	16.1	Наличие технических средств (способов) уничтожения образцов, черновиков, брака	1,0	0,8
	16.2	Наличие технических возможностей должной утилизации производственного брака	1,0	0,9
17	17.1	Наличие и использование средств маскировки, пломбирования и опечатывания	1,0	0,85
	17.2	Использование противокражных систем (например, радиометок) для контроля и учета сохранности продукции	0,8	0,8
18	18.1	Наличие и работоспособность ТСО, СКУД в помещениях с обработкой и хранением личных дел сотрудников	1,0	0,8
	18.2	Контроль по протоколам АРМ по сдаче под охрану помещений, посещения помещений уполномоченными лицами с обработкой и хранением личных дел сотрудников	0,75	1,0
19	19.1	Наличие и работоспособность ТСО, СКУД в помещениях с обработкой и хранением личных дел и персональных данных сотрудников	1,0	0,8
	19.2	Контроль по протоколам АРМ по сдаче под охрану помещений, посещения помещений уполномоченными лицами с обработкой и хранением личных дел и персональных данных сотрудников.	0,75	1,0
20	20.1	Контроль лиц, в служебное и не служебное время по служебным каналам связи (при согласии и необходимости)	0,7	0,6
	20.2	Контроль лиц, в служебное и не служебное время по их местоположению (GPS и т.д.) (при согласии и необходимости)	0,6	0,5
	20.3	Использование полиграфа (по возможности и необходимости)	1,0	0,9
	20.4	Использование (гласное и негласное) средств аудио и видеофиксации (при согласии и необходимости)	0,8	0,8
21	21.1	Психологическое тестирование сотрудников	1,0	0,7
	21.2	Использование полиграфа (по возможности и необходимости)	1,0	0,8
22	22.1	Тестирование знаний сотрудников специальными тестами и вводными задачами	1,0	0,8
23	23.1	Фактическое отсутствие или недостатки в технических средств обработки ПДн сотрудников, нарушения политики ИБ	0,8	0,8

Приложение 4

Таблица П4 – Характер проверочных мероприятий и способ получения частных организационных показателей оценки защищённости организационного канала утечки информации

№ частного показателя	Характер проверочных мероприятий, вопросы проверки (способы получения показателя)	Значение показателя M_{ij}
1	2	3
1.1	Наличие документа (утвержденного); Ознакомление с документом подчиненных; Ведется ли документация, предусмотренная нормативными документами; Соблюдаются ли основные положения документа (документальная проверка, опрос подчиненных, анализ протоколов ПО или негласная проверка)	Отсутствует или не выпол. -0; частично, менее 20% -0,2; менее 50% -0,5; менее 80% - 0,8% полностью -1
1.2	Наличие документа; Ознакомление с документом подчиненных; Соответствие кадрового состава (по квалификации и образованию) подразделения положению; Наличие должностных инструкций сотрудников подразделения; Знание сотрудниками своих обязанностей; Выполнение несвойственных подразделению функций (документальная проверка опрос, проверка знаний)	Отсутствует или не выполняется -0; выполняется частично, менее 20% -0,2; менее 50% -0,5; менее 80% - 0,8% полностью -1
1.3	Наличие документа (утвержденного) (да-1/нет-0); Соответствие информации в документе сфере деятельности и специфики предприятия (организации) (соответствует-1,0/частично соответствует-0,2¸0,8/не соответствует-0); Наличие информации, противоречащей ФЗ о КТ (да-0/нет-1); Ознакомление с документом подчиненных (сотрудников) (да-1/частично 0,2¸0,8/нет-0) (Документальная проверка)	Отсутствует или противоречит ФЗ - 0. В остальных случаях среднее значение оценок вопросов проверки
1.4	Наличие приказа о комиссии (да-1/нет-0); Ознакомление всех сотрудников-членов комиссии с приказом (да-1/нет-0); Наличие согласованных комиссией документов (все согласованы-1/частично-0,2¸0,8/нет согласованных-0); Регистрация согласования комиссией документов (да-1/частично-0,2¸0,8/нет-0); Знают ли о существовании комиссии сотрудники предприятия (да-1/частично-0,5/нет-0); Наличие отчетов (справок) и планов о деятельности комиссии (да-1/частично-0/нет-1) (Документальная проверка, опрос сотрудников)	Нет приказа или согласованных документов - 0. В остальных случаях среднее значение оценок вопросов проверки
1.5	Наличие документального подтверждения режима КТ (да-1/нет-0); Наличие утвержденного положения о разрешительной системе доступа к КТ (да-1/нет-0); Имеется ли документальное подтверждение режима КТ (уведомление сотрудников и их расписки о неразглашении, изменения в должностных инструкциях, положение о разрешительной системе допуска к КТ, перечень сведений, составляющих КТ, номенклатура должностей сотрудников, допущенных к КТ и т.д.) (да-1/частично-0,2¸0,8/нет-0); Информированы ли сотрудники организации о режиме КТ и основах обеспечения охраны КТ (да-1/частично-0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников)	Нет положения или подтверждающих документов - 0. В остальных случаях среднее значение оценок вопросов проверки
1.6	Наличие приказа об инвентаризации (да-1/нет-0); Наличие протоколов (актов) инвентаризации (да-1/нет-0); Ознакомление с актами и правилами инвентаризации должностных лиц-членов комиссии (да-1/нет-0); Выявлены ли недостатки учета и хранения при инвентаризации носителей и документов в ходе проверки (да-1/частично-0,2¸0,8/нет-1); Соблюдается ли периодичность и объём инвентаризации (да-1/нет-0); Имелись ли не устраненные замечания по предыдущим инвентаризациям (да-0/нет-1/частично-0,2¸0,8) (Документальная проверка, опрос сотрудников, инвентаризация)	Нет протоколов или актов, выявлена недостача - 0. В остальных случаях среднее значение оценок вопросов проверки

1.7	Выявлены ли факты хранения конфиденциальных документов и носителей вне предназначенных для этого помещений и сейфов (хранилищ) (да-0/нет-1); Имеются ли акты обследования помещений для хранения конфиденциальных документов и носителей (да-1/нет-0); Соблюдается ли периодичность обследования конфиденциальных документов и носителей (да-1/нет-0); Качество составления актов обследований (хорошее-1/удовлетворительное-0,5/не удовлетворительное-0); Устраняются ли замечания по актам обследования помещений (да-1/частично-0,2¸0,8/нет-0); Имеются ли замечания по требованиям к местам хранения конфиденциальных документов и носителей на момент проверки (нет замечаний-1/ не существенные замечания-0,7/критические (важные) замечания-0); Оборудовано ли помещение (и работоспособность) СКУД (да-1/нет-0); Оборудовано ли помещение (и работоспособность) ОТС (да-1/нет-0); Сдаются помещения только ответственными лицами или передается идентификатор другим лицам (да имеются факты-0/нет фактов-1); Соблюдается ли график охраны помещения (да-1/частично-0,2¸0,8/нет-0); Имеются ли факты когда документы и носители сотрудники забирают домой для работы дома. (да имеются факты-0/нет фактов-1); Всегда ли сотрудники запирают помещения (если нет СКУД) выходя из него и там имеется свободный доступ (да-0/нет-1) (Документальная проверка, опрос сотрудников, обследование помещений)	Если выявлены факты хранения конфиденц. документов и носителей вне предназначенных для этого помещений, не работоспособны СКУД или ОТС, имеются критические замечания при обследовании, носители сотрудники забирают домой (без разрешения), не запирают помещения оставляя их в свободном доступе -0. В остальных случаях среднее значение оценок вопросов проверки
1.8	Если используется ЭЦП или специальное ПО в СЭД имеются ли утвержденные инструкции по пользованию специализированным ПО (да-1/нет-0); Ознакомлены ли сотрудники и умеют ли они пользоваться данным ПО (да-1/ частично-0,2¸0,8/нет-0); Имеются ли нарушения в оформлении документов по сертификатам ЭЦП (да-1/частично-0,2¸0,8/нет-0); Ведутся ли предусмотренные журналы пользования ПО (если они предусмотрены) (да-1/частично-0,2¸0,8/нет-0); Пользуются ли пользователи чужой ЭЦП (да-0/нет-1) (Документальная проверка, опрос сотрудников, просмотр протоколов и сверка с журналами, негласная проверка)	Если нет инструкции, используются чужие ЭЦП – 0. В остальных случаях среднее значение оценок вопросов проверки
1.9	Имеются ли должностные инструкции у лиц, занимающихся конфиденциальным ДП (да-1/частично-0,2¸0,8/нет-0); Отражают ли должностные инструкции положения инструкции по обеспечению конфиденциального ДП (да-1/частично-0,2¸0,8/нет-0); Соответствие кадрового состава (по квалификации и образованию) должностным инструкциям (да-1/частично-0,2¸0,8/нет-0); Соблюдаются ли основные положения документа (да-1/частично-0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников, негласная проверка)	Если нет инструкций, фактически не исполняются инструкции-0. В остальных случаях среднее значение оценок вопросов проверки
1.10	Сдаются ли помещения с хранением конфиденциальных документов и носителей од охрану (не сдаются-0/ не всегда - 0,2¸0,8/всегда сдаются-1); Ведется ли журнал приема-сдачи помещений с КИ под охрану (или протокол работы АРМ) (ведется -1 /не ведется-0); Ведется ли журнал приема-выдачи ключей помещений с КИ (ведется-1 /не ведется-0); Опечатываются ли ответственными лицами помещения с хранением КИ документов и носителей (да-1/нет-0); Опечатываются ли ответственными лицами сейфы (шкафы) с хранением конфиденциальных документов и носителей (да-1/нет-0); Ведется ли журнал приема-выдачи носителей КИ сотрудникам (ведется -1/не ведется-0); Ведется ли журнал выдачи документов с КИ сотрудникам (ведется -1/не ведется-0); Ведется ли журнал работы с КИ на СВТ (или протокол) (да-1/нет-0) (Документальная проверка, опрос сотрудников, обследование, просмотр протоколов АРМ, негласная проверка)	Если помещения не сдаются под охрану, не ведутся журналы выдачи документов с КТ и носителей КТ - 0. В остальных случаях среднее значение оценок вопросов проверки

1.11	Используется ли в СЭД (СЗЭД) выход в глобальные информационные сети (нет-1/используется через сетевой экран с распределением доступа к ИР - 0,8/ через сетевой экран без распределения доступа -0,5/свободный выход-0) Используется ли в СЭД (СЗЭД) беспроводные сегменты корпоративных информационных сетей (нет-1/используются с защитой WPA-WPA2-0,9/используются без защиты-0); Используется ли в СЭД (СЗЭД) антивирусное ПО (да-1 /не достаточно используется -0,2¸0,8/ не используется-0); Постоянно ли обновляются в СЭД (СЗЭД) базы антивирусного ПО (не обновляются-0/ частично обновляются - 0,2¸0,8/обновляются своевременно-1); Телекоммуникации СЭД (СЗЭД) смонтированы «скрытым способом» (нет доступа посторонних лиц) (да-1/нет-0); Телекоммуникации СЭД (СЗЭД) проходят только через помещения, контролируемые предприятием (организацией), т.е. «охраняемые помещения» (да-1/нет-0); Для использования СЭД (СЗЭД) организован контроль доступа к ИР с процедурами аутентификации и идентификации на основе сертифицированных специализированных СЗИ (да-1/нет-0); Для использования СЭД (СЗЭД) организован контроль доступа к ИР с процедурами аутентификации и идентификации на основе возможностей ОС (конфигурирование пользователей ОС, если нет специализированных СЗИ) (да-1/нет-0); Осуществляется ли аудит ИБ для сегмента СЭД (СЗЭД) (да-1/нет-0); Имеются ли замечания и предложения по итогам аудита ИБ для сегмента СЭД (СЗЭД) (нет-1/не значительные -0,5/да-0); Соблюдается ли периодичность проведения аудита ИБ для сегмента СЭД (СЗЭД) (да-1/нет-0); Существует ли должность администратора безопасности корпоративной ЛВС (в т.ч. для сегмента СЭД (СЗЭД)) (да-1/нет-0); Утверждена ли политика ИБ на предприятии (в т. ч. для сегмента СЭД (СЗЭД)) (да-1/нет-0); Выполняются ли основные положения политики ИБ на предприятии (при ее наличии) (да-1/частично--0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников, обследование сегмента СЭД, просмотр протоколов, негласная проверка)	Если используется свободный выход СЭД (СЗЭД) в глобальные информационные сети, беспроводные сегменты без защиты, нет антивирусного ПО, нет политики ИБ или она не выполняется - 0. В остальных случаях среднее значение оценок вопросов проверки
1.12	Имеется ли не лицензионное ПО для сегмента СЭД (СЗЭД) (да-0/нет-1); Проводится категорирование ИС для сегмента СЭД (СЗЭД) (да-1/нет-0); Прошла ли процедура аттестации (если она необходима) для сегмента СЭД (СЗЭД) (да-1/нет-0); Полнота документального обеспечения сертификации, категорирования, аттестации объектов информатизации (если это требуется) (полное-1/ частичное -0,2¸0,8/в основном отсутствует-0) (Документальная проверка, обследование сегмента СЭД, просмотр протоколов)	Если есть не лицензионное ПО, нет аттестации объектов информатизации (если это требуется) - 0. В остальных случаях среднее значение оценок вопросов проверки
2.1	Наличие раздела об обеспечении конфиденциальности в договоре о проведении совместных работ (да-1/нет-0); Наличие раздела об ответственности при нарушении конфиденциальности в договоре о проведении совместных работ (да-1/нет-0); Наличие разрешительных распоряжение по допуску к КТ должностных лиц, представителей контрагентов (да-1/нет-0); Документальное подтверждение ознакомления должностных лиц, представителей контрагентов с КТ организации (в полном объеме-1/частичное-0,2¸0,8/нет-0); Соответствие характера конфиденциальной информации фактического ознакомления контрагентов с характером информацией, ознакомление с которой предусматривается совместным договором (соответствует-1/ частично -0,2¸0,8/ не соответствует -1) (Документальная проверка, опрос сотрудников)	Если нет раздела об обеспечении конфиденциальности в договоре о проведении совместных работ и ответственности, нет подтверждение ознакомления должностных лиц контрагентов с КТ - 0. В остальных случаях среднее значение оценок вопросов проверки
2.2	Наличие в инструкции по КП и ОР раздела по организации доступа только лиц, определенных совестным договором при наличии соответствующих распоряжений (да-1/нет-0) (Документальная проверка)	В соответствии с оценкой
2.3	Наличие в инструкции по КП и ОР раздела в части ограничения передвижения сторонних сотрудников по предприятию (да-1/нет-0) (Документальная проверка)	В соответствии с оценкой

2.4	Наличие в инструкции по КП и ОР раздела в части закрепления сопровождающих (ответственных за сопровождение) сотрудников предприятия за представителями контрагентов (да-1/нет-0); Контроль фактического выполнения сопровождения сотрудниками предприятия представителей контрагентов (да-1/частично-0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников)	Если нет в инструкции по КПиОР соответствующего раздела -0. В остальных случаях среднее значение оценок вопросов проверки
2.5	Наличие плана мероприятий по недопущению неформального общения лиц, допущенных к КТ разных организаций (да-1/нет-0) Фактическое выполнение плана мероприятий по недопущению неформального общения лиц, допущенных к КТ разных организаций (да-1/ частично-0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников)	Если нет плана мероприятий по недопущению неформ. общения -0. В остальных случаях среднее значение оценок вопросов проверки
2.6	Контроль лиц, находящихся в служебных командировках в служебное и не служебное время (да-1/частично-0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников)	В соответствии с оценкой
2.7	Имеется ли документальное подтверждение использования спец.связи и фельдъегерской связи (если требуется использование такой связи) (да-1/частично-0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников)	В соответствии с оценкой
3.1	При проведении совещаний (конференций и т.д.), в ходе которых обсуждаются вопросы конфиденциального характера, составляются ли планы защиты КТ при их проведении (да-1/ нет-0); Фактическое выполнение мероприятий планов проведения совещаний (конференций и т.д.), в ходе которых обсуждаются вопросы конфиденциального характера (да-1/частично-0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников)	Если нет плана мероприятий -0. В остальных случаях среднее значение оценок вопросов проверки
3.2	Предусматриваются ли планом проведения совещаний (конференций и т.д.), в ходе которых обсуждаются вопросы конфиденциального характера организация встречи, размещения приглашенных лиц по территории организации (да-1/частично-0,2¸0,8/нет-0) (Документальная проверка)	В соответствии с оценкой
3.3	Предусматриваются ли планом проведения совещаний (конференций и т.д.), в ходе которых обсуждаются вопросы конфиденциального характера организация встречи, мероприятия по досмотру (при необходимости) участников совещания и организация хранения личных вещей участников совещания (да-1/частично-0,2¸0,8/нет-0) (Документальная проверка)	В соответствии с оценкой
3.4	Предусматриваются ли планом проведения совещаний (конференций и т.д.), в ходе которых обсуждаются вопросы конфиденциального характера организация встречи, мероприятия по досмотру (при необходимости) участников совещания и организация хранения личных вещей участников совещания (да-1/частично-0,2¸0,8/нет-0); Проводятся ли инструктажи по обеспечению защиты КИ с участниками совещания (да-1/частично-0,2¸0,8/нет-0) (Документальная проверка)	Среднее значение оценок вопросов проверки
3.5	Проводится ли мероприятия по удалению из зала проведения совещаний ОТСС и ВТСС (по возможности) (да-1/частично-0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников)	В соответствии с оценкой
3.6	Проводится ли мероприятия по ограничению доступа приглашенных лиц по территории предприятия и в помещения проведения совещания (да-1/частично-0,2¸0,8/нет-0); Применяются ли какие-либо технические средства по ограничению доступа приглашенных лиц по территории предприятия и в помещения проведения совещания (да-1/частично-0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников)	Среднее значение оценок вопросов проверки
3.7	Осуществляется ли контроль рассматриваемых (строго по регламенту плана совещания) вопросов по ходу совещания (да-1/частично-0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников)	В соответствии с оценкой
3.8	Проведение мероприятий по недопущению неформального общения лиц, допущенных на совещание (да-1/частично-0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников)	В соответствии с оценкой
3.9	Устанавливаются ли агитационные материалы по недопущению обсуждения КТ в неустановленных помещениях (да-1/частично-0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников)	В соответствии с оценкой

3.10	Осуществляются ли проведение обследований («зачистка») помещений до и после совещаний (да-1/ нет-0); Составляется ли в полном объеме документация по проведению обследований («зачистки») помещений до и после совещаний (да-1/ нет-0) (Документальная проверка, опрос сотрудников)	Среднее значение оценок вопросов проверки
3.11	Осуществляется ли контроль (визуальный) и принятие мер при несанкционированном использовании участниками совещания технических средств (да-1/частично-0,2¸0,8/нет-0) (опрос сотрудников)	В соответствии с оценкой
3.12	Осуществляется ли обеспечение участников совещания раздаточным (рецензированным) материалом (да-1/ нет-0); Исключается ли возможность обеспечения участников совещания не санкционированным раздаточным материалом и носителями (да-1/ нет-0) (Документальная проверка, опрос сотрудников)	Если имеется несанкцион. материалы и носители - 0. В остальных случаях среднее значение оценок
3.13	Осуществляется ли обеспечение санкционированной рассылки материалов совещания участникам совещания (да-1/ нет-0); Исключается ли возможность обеспечения несанкционированной рассылки материалов совещания участникам совещания (да-0/ нет-0) (Документальная проверка, опрос сотрудников)	Если имеется несанкцион. рассылка - 0. В остальных случаях среднее значение оценок вопросов проверки
3.14	Используются ли (при необходимости) сертифицированные ТСЗИ, (аттестованные помещения) при проведении совещаний (да-1/ нет-0) (Документальная проверка)	В соответствии с оценкой
4.1	Порядок принятия решений о зарубежном выезде соответствует ли требованиям нормативных документов (да-1/частично-0,2¸0,8/нет-0) (Документальная проверка)	В соответствии с оценкой
4.2	Имеются ли обязательств сотрудника о неразглашении КТ (да-1/ нет-0) (Документальная проверка)	В соответствии с оценкой
4.3	Проводились ли (документальное подтверждение) инструктажи с сотрудниками при зарубежных выездах (да-1/ нет-0) (Документальная проверка)	В соответствии с оценкой
4.4	Проведение мероприятий по недопущению неформального общения лиц, выезжающих за рубеж (да-1/частично-0,2¸0,8/нет-0); Имеются ли у лиц, выезжающих за рубеж в стране выезда родственники, знаковые, коллеги (да-0/нет-1) (Документальная проверка, опрос сотрудников)	Если имеются знакомые (друзья, родственники) - 0. В остальных случаях - среднее значение оценок
4.5	Осуществляется ли отслеживание контактов (по возможности и необходимости) сотрудников за границей (да-1/частично-0,2¸0,8/нет-0) (опрос сотрудников)	В соответствии с оценкой
4.6	Осуществляется ли сопровождение (по возможности и необходимости) делегации или индивидуально сотрудников за границей (да-1/ нет-0); Осуществляется ли негласный контроль (по возможности и необходимости) делегации или индивидуально сотрудников за границей (да-1/ нет-0) (опрос сотрудников)	Среднее значение оценок вопросов проверки
4.7	Осуществляется ли «зачистка» (по возможности и необходимости) багажа и личных вещей сотрудников до и после приезда (да-1/ нет-0) (опрос сотрудников)	В соответствии с оценкой
4.8	Осуществляется ли контроль лиц, находящихся в служебных командировках в служебное и не служебное время (да-1/частично-0,2¸0,8/нет-0) (опрос сотрудников)	В соответствии с оценкой
4.9	Осуществляется ли контроль отчета по выезду (если он служебный) и подтверждающих документов (командировка, путевка, билеты, визы, отметки в паспортах и т.д.) (да-1/частично-0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников)	В соответствии с оценкой
5.1	Имеется ли постоянно действующая экспертная комиссия (ПДЭК) по контролю исходящей информации при публикационной деятельности (да-1/ нет-0); Имеются ли документальные акты (отчеты, справки) по деятельности комиссии (да-1/ нет-0) (Документальная проверка, опрос сотрудников)	Если нет приказа о комиссии и актов-0. В остальных случаях среднее значение оценок вопросов проверки
5.2	Ознакомлены ли сотрудники организации о порядке осуществления издательской, рекламной и публикационной деятельности (да-1/ нет-0); Существуют ли согласованные планы взаимодействия организации со СМИ (да-1/ нет-0) (Документальная проверка, опрос сотрудников)	Если не ознакомлены и нет плана-0. В остальных случаях среднее значение оценок вопросов проверки
5.3	Есть ли отдельные должностные лица (подразделения) по взаимодействию со СМИ (да-1/ нет-0) (Документальная проверка)	В соответствии с оценкой

5.4	Качество должностных инструкцию должностных лиц по взаимодействию со СМИ (их взаимодействие с ПДЭК) (высокое-1 /среднее 0,2¸0,8/низкое-0) (Документальная проверка)	В соответствии с оценкой
5.5	Осуществляется ли анализ публикаций, рекламных материалов и др. исходящих документов со стороны РСП (СБ) организации (да-1/частично-0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников)	В соответствии с оценкой
5.6	Осуществляется ли взаимодействие (при необходимости) с другими предприятиями и организациями по вопросам открытого опубликования материалов, содержащих КТ о проводимых совместных и других работах (да-1/ нет-0) (Документальная проверка, опрос сотрудников)	В соответствии с оценкой
5.7	Повторяется исполнение п.1.5	В соответствии с пунктом 1.5
5.8	Имеются ли ограничения допуска к КТ лиц ответственных за взаимодействие со СМИ и рекламу на предприятии (да-1/ нет-0) (Документальная проверка, опрос сотрудников)	В соответствии с оценкой
5.9	Соблюдается ли недопущение в режимные и выделенные помещения экскурсий, журналистов и др. (да-1/частично-0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников, негласные проверки)	В соответствии с оценкой
6.1	Наличие положения об отделе ТЗИ (при необходимости) и инструкции по ТЗИ (да-1/ нет-0); Фактическое исполнение требований инструкции по ТЗИ (да-1/частично-0,2¸0,8/нет-0) (Документальная проверка)	Если нет положения и фактического исполнения -0. В остальных случаях среднее значение
6.2	Наличие утвержденного перечня сведений, КТ, передаваемой иностранным государствам (их представителям и организациям) (да-1/ нет-0); Контроль передачи информации строго по перечню разрешенных к передаче сведений и только в необходимом в рамках договора объеме (соответствует перечню-1/ частично соответствует- 0,2¸0,8/ не соответствует-0) (Документальная проверка)	Если нет перечня и контроля - 0. В остальных случаях среднее значение оценок
6.3	Имеются ли разрешительные федеральные нормативные межгосударственные документы для передачи КТ (при необходимости) (да-1/ нет-0) (Документальная проверка)	В соответствии с оценкой
6.4	Имеется ли договор о проведении совместных работ с иностранными партнерами для передачи КТ (да-1/ нет-0); Имеется ли в договоре о проведении совместных работ с иностранными партнерами и при передаче КТ раздел об обеспечении КТ (да-1/ нет-0) (Документальная проверка)	Если нет договора и фактического исполнения -0. В остальных случаях среднее значение
6.5	Назначены ли ответственные лица за информационный обмен КТ с иностранными партнерами (да-1/ нет-0) (Документальная проверка)	В соответствии с оценкой
6.6	Проводились ли инструктажи с сотрудниками организации по обеспечению КИ при сотрудничестве с иностранными партнерами (да-1/ нет-0) (Документальная проверка, опрос сотрудников)	В соответствии с оценкой
6.7	Имеются ли расписки сотрудников о неразглашении КТ при взаимодействии с иностранными партнерами (да-1/ нет-0) (Документальная проверка)	В соответствии с оценкой
6.8	Проведение мероприятий по недопущению неформального общения лиц, допущенных к КИ с иностранными партнерами (да-1/ частично0,2¸0,8/нет-0); Имеются ли у лиц, допущенных к КИ родственники, знаковые, коллеги из страны, откуда прибыли иностранными партнерами (да-1/нет-0) (Документальная проверка, опрос сотрудников)	Среднее значение оценок вопросов проверки
6.9	Проводятся ли мероприятия по отслеживанию контактов (по возможности и необходимости) сотрудников предприятия и иностранных представителей (да-1/ нет-0) (Документальная проверка)	В соответствии с оценкой
6.10	Контролируется ли передача иностранным партнерам конфиденциальных сведений со стороны ПДЭК (да-1/ нет-0) (Документальная проверка)	В соответствии с оценкой
6.11	Имеется ли документальное подтверждение использования спец.связи и фельдъегерской связи (если требуется использование такой связи) (да-1/ нет-0) (Документальная проверка)	В соответствии с оценкой
7.1	Повторяется исполнение п.6.1 для научных исследований, НИР и ОКР	В соответствии с пунктом 6.1

7.2	Имеется ли не лицензионное ПО при научных исследованиях, НИР и ОКР (да-0/нет-1); Используется ли (при необходимости) сертифицированное ПО при научных исследованиях, НИР и ОКР (да-1/нет-0); Проводится ли категорирование и аттестация (при необходимости) ОИ при работе НИР и ОКР (да-1/нет-0); Полнота документального обеспечения сертификации, категорирования, аттестации ИС и объектов информатизации (если это требуется) (полное-1/ частичное- 0,2¸0,8/ отсутствует-0) (Документальная проверка)	Среднее значение оценок вопросов проверки
7.3	Имеется ли инструкция (раздел общей инструкции по обеспечению КТ при научных исследованиях, НИР и ОКР (да-1/нет-0); Фактически исполняются принципиальные положения инструкции по обеспечению КТ при научных исследованиях, НИР и ОКР (полное-1/ частичное- 0,2¸0,8/ отсутствует-0) (Документальная проверка, опрос сотрудников)	Если нет инструкции и фактического исполнения -0. В остальных случаях среднее значение оценок вопросов проверки
7.4	Имеется ли в инструкции по ПДЭК положений по контроля обеспечения КИ при проведении научных исследований, НИР и ОКР (да-1/нет-0); Фактически осуществляется ли контроль исходящей документации по научным исследованиям, НИР и ОКР со стороны ПДЭК (да-1/нет-1) (Документальная проверка, опрос сотрудников)	Если нет инструкции и фактического исполнения -0. В остальных случаях среднее значение оценок вопросов проверки
7.5	Имеется ли документация по контролю ведения патентной документации и лицензионных договоров, юридическое сопровождение патентной работы и охране интеллектуальной собственности (полное-1/ частичное- 0,2¸0,8/ отсутствует-0) (Документальная проверка)	В соответствии с оценкой
7.6	Имеется ли разделение сфер разработки между сотрудниками и отделами (полная информация о разработке должна быть только у ограниченного количества руководителей) (полное-1/ частичное- 0,2¸0,8/ отсутствует-0) (Документальная проверка)	В соответствии с оценкой
7.7	Содержаться ли в инструкции о КПиОР, допуск в определенные помещения только лиц, допущенных к НИР и ОКР (база данных СКУД) (да-1/нет-1) (Документальная проверка, опрос сотрудников, проверка протоколов СКУД)	В соответствии с оценкой
7.8	Выявлены ли факты хранения КИ документов по науке, НИР и ОКР и носителей вне предназначенных для этого помещений и сейфов (хранилищ) (да-0/нет-1); Имеются ли акты обследования помещений для хранения конфиденциальных документов и носителей по науке, НИР и ОКР (да-1/нет-0); Имеются ли замечания к местам хранения КИ документов и носителей (нет замечаний-1/ не существенные - 0,2¸0,8/критические (важные) замечания-0); Оборудовано ли помещение хранения КТ (и работоспособность) СКУД (да-1/нет-0); Оборудовано ли помещение (и работоспособность) хранения КИ ОТС (да-1/нет-0); Сдаются помещения только ответственными лицами или передается идентификатор другим лицам (да имеются факты-0/нет фактов-1); Имеются ли факты когда документы КИ и носители сотрудники забирают домой (да имеются факты-0/нет фактов-1); Всегда ли сотрудники запирают помещения (если нет СКУД) выходя из него и там никто не остается (да-1/нет-0) (Документальная проверка, опрос сотрудников, проверка протоколов ОТС и СКУД)	Если хранятся документы и носители в неустановленном месте, не работоспособны ОТС и СКУД, передаются идентификаторы и забирают домой носители (без разрешения) -0. В остальных случаях среднее значение оценок вопросов проверки
7.9	Осуществляется ли передача информации по НИР и ОКР по открытым каналам связи и телекоммуникаций за пределами режимных помещений (да-0/нет-1) (опрос сотрудников)	В соответствии с оценкой
7.10	Используется ли ТСЗИ от утечки по техническим каналам (при необходимости) при проведении научных исследований, НИР и ОКР (да-1/нет-0) (Документальная проверка, опрос сотрудников, проверка протоколов)	В соответствии с оценкой
7.11	Повторяется исполнение п.1.6 для информационных документов и изделий (образцов, черновиков, брака и т.д.) содержащих КТ по НИР и ОКР	В соответствии с пунктом 1.6

7.12	Имеется ли оборудование для уничтожения и утилизации черновиков, брака и отходов производства содержащих КТ по НИР и ОКР (да-1/нет-0); Создана ли приказом комиссия для уничтожения и утилизации черновиков, брака и отходов производства содержащих КТ по НИР и ОКР (да-1/нет-0); Фактически обеспечивается ли требуемое уничтожения и утилизации черновиков, брака и отходов производства содержащих КТ по НИР и ОКР (да-1/нет-0) (Документальная проверка, опрос сотрудников, негласная проверка)	Если не обеспечивается требуемое уничтожение и утилизации черновиков, брака и отходов производства содержащих КТ по НИР и ОКР -0. В остальных случаях среднее значение оценок вопросов проверки
7.13	Осуществляется ли контроль по протоколам АРМ СКУД и ОТС посещений помещений, сдаче под охрану режимных помещений уполномоченными лицами (да-1/частично -0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников, проверка протоколов)	В соответствии с оценкой
7.14	Имеются ли документальные свидетельства работы с КТ по науке, НИР и ОКР, по соответствующим журналам (по внутренним распорядительным документам) (да-1/частично -0,2¸0,8/нет-0)	В соответствии с оценкой
7.15	Повторяется исполнение п.п.1.11 для КТ по научным исследованиям, НИР и ОКР	В соответствии с пунктом 1.11
7.16	Имеется ли документальное подтверждение использования спец.связи и фельдъегерской связи (если требуется использование такой связи) для КИ по научным исследованиям, НИР и ОКР (да-1/ нет-0)	В соответствии с оценкой
8.1	Имеется ли в инструкции по КПиОР раздел по порядку организации доступа на территорию и в определенные помещения сотрудников территориальных инспекторских и надзорных органов только с сопровождающими лицами (да-1/ нет-0) (Документальная проверка)	В соответствии с оценкой
8.2	Проводятся ли инструктажи сотрудников о порядке допуска и ознакомления с документацией представителей инспекторских и надзорных органов (да-1/частично -0,2¸0,8/нет-0) (Документальная проверка)	В соответствии с оценкой
8.3	Определено ли инструкциями обеспечение передачи материалов только при условиях: на законных основаниях; только с разрешения руководства; только в необходимых объемах; только уполномоченным лицам под расписку (да-1/частично -0,2¸0,8/нет-0); Фактически соблюдается ли обеспечение передачи материалов только при условиях: на законных основаниях; только с разрешения руководства; только в необходимых объемах; только уполномоченным лицам под расписку (да-1/частично -0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников)	Среднее значение оценок вопросов проверки
8.4	Определено ли инструкциями обеспечение защиты электронных каналов передачи информации (при их наличии) (да-1/частично -0,2¸0,8/нет-0); Фактически соблюдается ли обеспечение защиты электронных каналов передачи информации (при их наличии) (да-1/частично -0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников)	Если нет инструкции и фактического исполнения - 0. В остальных случаях среднее значение оценок вопросов проверки
8.5	Обеспечивается ли при передаче информации защита персональных данных сотрудников в соответствии с федеральными законодательными актами (да-1/частично -0,2¸0,8/нет-0) (Документальная проверка)	В соответствии с оценкой
8.6	Повторяется исполнение п.1.3 для КТ переданной в территориальные инспекторские и надзорные органы	В соответствии с пунктом 1.3
8.7	Повторяется исполнение п.1.5 для КТ переданной в территориальные инспекторские и надзорные органы	В соответствии с пунктом 1.5
8.8	Осуществляется ли контроль по протоколам АРМ СКУД и просмотр записей СВН посещений помещений предприятия сотрудниками территориальных инспекторских и надзорных органов (да-1/частично -0,2¸0,8/нет-0) (Документальная проверка, анализ протоколов)	В соответствии с оценкой
8.9	Повторяется исполнение п. 7.16 для КТ, переданной в территориальные инспекторские и надзорные органы	В соответствии с пунктом 7.16
9.1	Повторяется исполнение п..2.2	В соответствии с пунктом 2.2

9.2	Наличие договора с ЧАО или гос.службой (например, с вневедомственной охраной) по охране объекта и осуществлении КПиОР (наличие в штате собственной службы физического реагирования) (да-1/нет-0); Фактическое качество исполнения договора с ЧАО или гос.службой по охране объекта и осуществлении КПиОР (хорошее-1/ удовлетворительное - 0,2¸0,8/ не удовлетворительное-0) (Документальная проверка, опрос, негласная проверка)	Если нет договора и фактического исполнения -0. В остальных случаях среднее значение оценок вопросов проверки
9.3	Наличие утвержденных должностных инструкций сотрудников охраны (да-1/нет-0); Ознакомление с должностными инструкциями сотрудников охраны (да-1/нет-0); Качество знаний сотрудниками охраны своих должностных инструкций (хорошее-1/ удовлетворительное - 0,2¸0,8/ не удовлетворительное-0) (Документальная проверка, опрос)	Если нет инструкций -0. В остальных случаях среднее значение
9.4	Наличие инструкции о сдаче помещений под охрану (да-1/нет-0); Наличие инструкции о хранении ключей (да-1/нет-0) (Документальная проверка)	Среднее значение оценок вопросов проверки
9.5	Производится ли в полном объеме ведение исполнительской документации (протоколов АРМ) при осуществлении КПиОР (да/частично/нет) (Документальная проверка)	В соответствии с оценкой
9.6	Наличие с СБ специалистов в данной области (да-1/нет-0) (Документальная проверка)	В соответствии с оценкой
9.7	Имеется ли сертификация оборудования и технических средств обеспечения КПиОР (да-1/нет-0) (Документальная проверка)	В соответствии с оценкой
9.8	Имеется ли договор на монтаж технических средств охраны, СКУД, СВН и др. оборудования КПР (да-1/нет-0); Имеется ли лицензия (и опыт работы) организации, осуществляющей монтаж технических средств охраны, СКУД, СВН и др. оборудования КПР (да-1/нет-0) (Документальная проверка)	Нет договора и проекта-0. В остальных случаях среднее значение оценок вопросов проверки
9.9	Имеется ли договор проведения технического надзора за монтажными и пуско-наладочными работами (со стороны охранной организации) (да-1/нет-0) (Документальная проверка)	В соответствии с оценкой
9.10	Соблюдение периодичности и объемов регламентов при эксплуатационно-техническом обслуживании технических средств КПиОР (СВН, ОТС, СКУД и др.) (да-1/частично - 0,2¸0,8/нет-0); Ведется ли эксплуатационно-техническая документация при эксплуатационно-техническом обслуживании технических средств КПР (СВН, ОТС, СКУД и др.) (да-1/частично - 0,2¸0,8/нет -0) (Документальная проверка)	Среднее значение оценок вопросов проверки
9.11	Осуществляется ли контроль по протоколам АРМ СКУД и ОТС посещений помещений, сдаче под охрану помещений со стороны СБ предприятия (да-1/частично - 0,2¸0,8/нет -0) (Документальная проверка, контроль протоколов АРМ)	В соответствии с оценкой
9.12	Проводятся ли плановые и внеплановые проверки физической охраны предприятия (соблюдение дислокации, экипировки, действий при реагировании на тревожные ситуации), проведение тренировок и учений физической охраны (да-1/частично - 0,2¸0,8/нет -0); Проводятся ли плановые и внеплановые проверки физической охраны предприятия (соблюдение дислокации, экипировки, действий при реагировании на тревожные ситуации), проведение тренировок и учений физической охраны (да-1/частично - 0,2¸0,8/нет -0); Имеются ли замечания по учениям и тренировкам (да-1/частично - 0,2¸0,8/нет -0); Устраняются ли замечания по учениям и тренировкам (да-1/частично - 0,2¸0,8/нет -0) (Документальная проверка, контроль протоколов АРМ, опрос сотрудников, негласная проверка)	Среднее значение оценок вопросов проверки
10.1	Повторяется исполнение п.2.2	В соответствии с пунктом 2.2
10.2	Повторяется исполнение п.9.2 для объектового режима	В соответствии с пунктом 9.2
10.3	Повторяется исполнение п.9.3 для объектового режима	В соответствии с пунктом 9.3
10.4	Повторяется исполнение п.9.6 для объектового режима	В соответствии с пунктом 9.6
10.5	Обеспечивается ли защита персональных данных посетителей (не спрашивается ли лишняя информация) (да-1/нет-0) (Документальная проверка, опрос сотрудников)	В соответствии с оценкой

10.6	Повторяется исполнение п.9.4 для объектового режима	В соответствии с пунктом 9.4
10.7	Повторяется исполнение п.9.5 для объектового режима	В соответствии с пунктом 9.5
10.8	Повторяется исполнение п.9.7 для объектового режима	В соответствии с пунктом 9.7
10.9	Повторяется исполнение п.9.8 для объектового режима	В соответствии с пунктом 9.8
10.10	Повторяется исполнение п.9.9 для объектового режима	В соответствии с пунктом 9.9
10.11	Повторяется исполнение п.9.10 для объектового режима	В соответствии с пунктом 9.10
10.12	Повторяется исполнение п.9.11 для объектового режима	В соответствии с пунктом 9.11
10.13	Повторяется исполнение п.9.12 для объектового режима	В соответствии с пунктом 9.12
11.1	Повторяется исполнение п.9.8 для СКУД.	В соответствии с пунктом 9.8
11.2	Повторяется исполнение п.9.9 для СКУД.	В соответствии с пунктом 9.9
11.3	Наличие проектно-сметной документации по СКУД (да-1/нет-0) (Документальная проверка)	В соответствии с оценкой
11.4	Повторяется исполнение п.9.2 для СКУД.	В соответствии с пунктом 9.2
11.5	Имеются ли акты периодического обследования состояния технических средств СКУД (да-1/нет-0); Имеются ли замечания (и устраняются ли они) по актам периодического обследования состояния технических средств СКУД, устранение выявленных ранее недостатков (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка)	Если нет актов 0. В остальных случаях среднее значение
11.6	Выявление по результатам обследований СКУД ошибок монтажа, программирования и уязвимых мест проходов СКУД (да-0/нет-1). Устранены ли на момент проверки замечания по результатам обследований СКУД ошибок монтажа, программирования и уязвимых мест проходов в СКУД (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, обследование СКУД и АРМ СКУД)	Если выявлены ошибки 0. В остальных случаях среднее значение
11.7	Осуществляется ли своевременная смена пропусков, идентификаторов, паролей и своевременная ротации информации БД (да-1/нет-0) (проверка протоколов и БД СКУД)	В соответствии с оценкой
11.8	Имеется ли инструкция по использованию СКУД, назначение ответственных за эксплуатацию СКУД и ведение БД (да-1/нет-0); Назначены ли ответственные лица за эксплуатацию СКУД (да-1/нет-0). Назначены ли ответственные лица за ведение баз данных СКУД (да-1/нет-0) (Документальная проверка)	Среднее значение оценок вопросов проверки
11.9	Внесены ли пункты по СКУД в должностные обязанности сотрудников, эксплуатирующих СКУД (да-1/нет-0) (Документальная проверка)	В соответствии с оценкой
11.10	Повторяется исполнение п.9.12 для СКУД	В соответствии с пунктом 9.12
11.11	Повторяется исполнение п.9.11 для СКУД	В соответствии с пунктом 9.11
12.1	Повторяется исполнение п.9.8 для ОТС	В соответствии с пунктом 9.8
12.2	Имеется ли договор проведения технического надзора за монтажными и пуско-наладочными работами (со стороны охранной организации) (да-1/нет-0); Наличие проектно-сметной документации по ОТС (да-1/нет-0) (Документальная проверка)	Среднее значение оценок вопросов проверки
12.3	Повторяется исполнение п.9.2 для ОТС	В соответствии с пунктом 9.2
12.4	Повторяется исполнение п.9.10 для ОТС	В соответствии с пунктом 9.10
12.5	Повторяется исполнение п.12.5 для ОТС	В соответствии с пунктом 12.5

12.6	Повторяется исполнение п.12.6 для ОТС	В соответствии с пунктом 12.6
12.7	Повторяется исполнение п.12.7 для ОТС	В соответствии с пунктом 12.7
12.8	Повторяется исполнение п.12.8 для ОТС	В соответствии с пунктом 12.8
12.9	Повторяется исполнение п.12.9 для ОТС	В соответствии с пунктом 12.9
12.10	Повторяется исполнение п.12.10 для ОТС	В соответствии с пунктом 12.10
12.11	Повторяется исполнение п.12.11 для ОТС	В соответствии с пунктом 12.11
13.1	Используются ли ТСЗИ в СПИ если они должны быть по требованию документов (да-1/нет-0); Находятся ли средства ТЗИ в исправном состоянии (да-1/нет-0); Фактически используются ли ТСЗИ защиты СПИ (да-1/частично - 0,2¸0,8/нет-0); Документально подтверждается ли использование ТЗИ при передаче КТ по каналам СПИ (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, проверка работоспособности ТЗИ, контроль протоколов, опрос сотрудников)	Если нет ТЗИ или они не исправны -0. В остальных случаях среднее значение оценок вопросов проверки
13.2	Повторяется исполнение п. 6.1 по содержанию для передачи КТ по СПИ	В соответствии с пунктом 6.1
13.3	Повторяется исполнение п.5.1 по содержанию для передачи КТ по СПИ	В соответствии с пунктом 5.1
13.4	Повторяется исполнение п. 9.8 по содержанию для передачи КТ по СПИ	В соответствии с пунктом 9.8
13.5	Наличие с СБ специалистов в данной области (да-1/нет-0)	В соответствии с оценкой
13.6	Повторяется исполнение п.7.2 по содержанию для передачи КТ по СПИ	В соответствии с пунктом 7.2
13.7	Наличие всех соответствующих разрешительных документов УЦ (д-1а/нет-0); Имеется ли инструкция по использованию ЭЦП (да-1/нет-0); Ознакомление с инструкцией сотрудников (да-1/нет-0) (при требованиях по использованию ЭЦП) (Документальная проверка)	Среднее значение оценок вопросов проверки
13.8	Повторяется исполнение п. 1.11для каналов передачи информации и СПИ	В соответствии с пунктом 1.11
13.9	Имеются ли должностные инструкции у лиц, занимающихся передачей КТ по каналам связи и СПИ (да-1/частично-0,2¸0,8/нет-0); Соответствие кадрового состава (по квалификации и образованию) должностным инструкциям (да-1/частично- 0,2¸0,8/нет-0); Соблюдаются ли основные положения документа (да-1/частично - 0,2¸0,8/нет-0); Наличие плана мероприятий по обучению персонала закрытию каналов (да-1/нет-0); Фактическое выполнение плана мероприятий по обучению персонала закрытию каналов (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, контроль протоколов, опрос сотрудников, негласная проверка)	Если нет инструкций, не соблюдаются требования -0. В остальных случаях среднее значение оценок вопросов проверки
13.10	Наличие протоколов работы закрытия информации в каналах связи (да-1/нет-0) (Контроль протоколов)	В соответствии с оценкой
13.11	Наличие средств криптозащиты в каналах связи (если это требуется) (да-1/нет-0). Работоспособность СКЗИ (да-1/нет-0); Соответствие систем СКЗИ требованиям ФСБ (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, контроль протоколов, проверка работоспособности СКЗИ)	Если нет СКЗИ, или они не работоспособны 0. В остальных случаях среднее значение оценок вопросов проверки
14.1	Проведение аттестационных мероприятий объектов информатизации (ОИ) (если требуется) организацией, имеющей соответствующие лицензии (да-1/нет-0); Наличие должной сопроводительной документации (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка)	Если нет аттестации-0. В остальных случаях среднее значение оценок вопросов проверки
14.2	Осуществлялась ли проверки эффективности ТСЗИ от утечки по техническим каналам (да-1/нет-0) (Документальная проверка)	В соответствии с оценкой
14.3	Повторяется исполнение п. 9.8 для ТСЗИ от утечки по техническим каналам	В соответствии с пунктом 1.11

14.4	Наличие с СБ специалистов в данной области (да-1/нет-0) (Документальная проверка)	В соответствии с оценкой
14.5	Повторяется исполнение п.7.2 для ТСЗИ от утечки по техническим каналам	В соответствии с пунктом 7.2
14.6	Повторяется исполнение п.1.11 для ТСЗИ от утечки по техническим каналам	В соответствии с пунктом 1.11
14.7	Наличие инструкции по эксплуатации ТСЗИ (при необходимости их использования) (да-1/нет-0); Наличие методики поиска закладных устройств (да-1/нет-0) (Документальная проверка)	Если нет инструкций-0. В остальных случаях среднее значение оценок вопросов проверки
14.8	Имеются ли должностные инструкции у лиц, занимающихся ТСЗИ (да-1/частично-0,2¸0,8/нет-0); Соответствие кадрового состава (по квалификации и образованию) должностным инструкциям (да-1/частично - 0,2¸0,8/нет-0); Соблюдаются ли основные положения документа (да-1/частично--0,2¸0,8/нет-0); Наличие плана мероприятий по обучению персонала по защите от утечки информации по техническим каналам (да-1/нет-0); Фактическое выполнение плана мероприятий по обучению персонала по защите от утечки информации по техническим каналам (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников, негласная проверка)	Если нет инструкции и планов обучения-0. В остальных случаях среднее значение оценок вопросов проверки
14.9	Повторяется исполнение п. 13.10	В соответствии с пунктом 13.10
14.10	Ведение документации комиссиями по категорированию ОИ, конфиденциальности, ПДЭК и т.д. (при необходимости) (да-1/нет-0) (Документальная проверка)	В соответствии с оценкой
14.11	Наличие положения об отделе ТЗИ (да-1/нет-0); Наличие инструкции по использованию ТЗИ (да-1/нет-0); Исполнение требований данных документов (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников, негласная проверка)	Если нет инструкции и фактического исполнения-0. В остальных случаях среднее значение
14.12	Наличие необходимой исполнительской документации использования ТСЗИ (да-1/частично - 0,2¸0,8/нет-0); Соответствие наполнения документации реальному использованию (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников, негласная проверка)	Среднее значение оценок вопросов проверки
14.13	Наличие регламента по проведению обслуживания и проверки ТСЗИ (да-1/нет-0); Соблюдение регламента по обслуживанию и проверке ТСЗИ (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников, негласная проверка)	Среднее значение оценок вопросов проверки
15.1	Повторяется исполнение п.1.1	В соответствии с пунктом 1.1
15.2	Наличие инструкции об обеспечении конфиденциальности КТ (да-1/нет-0); Соответствие инструкции СТР-К (да-1/частично - 0,2¸0,8/нет-0); Ознакомление с инструкцией сотрудников (да-1/частично - 0,2¸0,8/нет-0); Фактическое исполнение инструкции (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников, негласная проверка)	Если нет инструкции и фактического исполнения-0. В остальных случаях среднее значение
15.3	Повторяется исполнение п.1.3.	В соответствии с пунктом 1.3
15.4	Повторяется исполнение п.п.1.4	В соответствии с пунктом 1.4
15.5	Повторяется исполнение п.1.5	В соответствии с пунктом 1.5
15.6	Повторяется исполнение п.1.6	В соответствии с пунктом 1.6
15.7	Повторяется исполнение п.1.7	В соответствии с пунктом 1.7
15.8	Повторяется исполнение п.1.9	В соответствии с пунктом 1.9

15.9	Наличие документов (актов) уничтожения и утилизации КИ и носителей КИ (да-1/нет-0); Наличие ответственного сотрудника (да-1/нет-0); Соответствие документов (актов) реальному положению дел (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников, негласная проверка)	Если нет актов - 0. В остальных случаях среднее значение
15.10	Наличие ответственного сотрудника по контролю за уничтожением черновиков, образцов, использованных носителей (да-1/нет-0); Наличие комиссии по оценке качества утилизации (да-1/нет-0); Наличие актов утилизации (да-1/нет-0) (Документальная проверка)	Если нет актов - 0. В остальных случаях среднее значение
16.1	Наличие раздела в инструкции по обеспечению конфиденциальности КТ (да-1/нет-0) (Документальная проверка)	В соответствии с оценкой
16.2	Повторяется исполнение п.15.9	В соответствии с пунктом 15.9
16.3	Повторяется исполнение п.1.9 для утилизации брака	В соответствии с пунктом 1.9
16.4	Повторяется исполнение п.15.10 для утилизации брака	В соответствии с пунктом 15.10
16.5	Наличие договоров со сторонними организациями по утилизации брака (при отсутствии собственных возможностей) (да-1/нет-0) (Документальная проверка)	В соответствии с оценкой
17.1	Повторяется исполнение п.5.2. для транспортировки и хранения продукции конфиденциального характера	В соответствии с пунктом 5.2
17.2	Повторяется исполнение п.1.9	В соответствии с пунктом 1.9
17.3	Повторяется исполнение п.6.1	В соответствии с пунктом 6.1
17.4	Наличие инструкции по КПиОР для хранения и транспортирования продукции конфиденциального характера (если требуется) (да-1/нет-0) (Документальная проверка)	В соответствии с оценкой
17.5	Наличие требований по таре, маскировке, маркировке и т.д. (да-1/нет-0); Соблюдение требований (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка)	Среднее значение оценок вопросов проверки
17.6	Повторяется исполнение п.1.6 для продукции конфиденциального характера	В соответствии с пунктом 1.6
18.1	Ознакомление с инструкциями федеральных ведомственных и др. вышестоящих организаций по приему на работу сотрудников (да-1/частично - 0,2¸0,8/нет-0); Соблюдение инструкций по приему на работу (да-1/нет-0) (Документальная проверка, опрос сотрудников)	Среднее значение оценок вопросов проверки
18.2	Повторяется исполнение п.18.1 для внутренних организационно распорядительных требований	В соответствии с пунктом 18.1
18.3	Повторяется исполнение п.1.1 для КТ	В соответствии с пунктом 1.1
18.4	Повторяется исполнение п.1.3	В соответствии с пунктом 1.3
18.5	Повторяется исполнение п.1.5	В соответствии с пунктом 1.5
18.6	Повторяется исполнение п.1.9	В соответствии с пунктом 1.9
18.7	Наличие расписок сотрудников о неразглашении КТ (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка)	В соответствии с оценкой
18.8	Наличие утвержденной номенклатуры допущенных к КТ должностей (да-1/нет-0) (Документальная проверка)	В соответствии с оценкой
18.9	Наличие личных дел сотрудников (если требуется) (да-1/нет-0); Своевременно обновляемая информация в личных делах сотрудников (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка)	Среднее значение оценок вопросов проверки
18.10	Наличие материалов анкет, опросов, обследований сотрудников (да-1/нет-0) (Документальная проверка)	В соответствии с оценкой
18.11	Соответствие квалификационных требований (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка)	В соответствии с оценкой

18.12	Соответствие требований по сохранности ПДн ФЗ-152 (да-1/частично - 0,2¸0,8/нет-0)	В соответствии с оценкой
18.13	Повторяется исполнение 1.6 для личных дел сотрудников, допущенных к КТ	В соответствии с пунктом 1.6
18.14	Работа аттестационных и кадровых комиссий в организации (да-1/нет-0); Наличие сопроводительных документов работы комиссий (да-1/нет-0) (Документальная проверка)	Среднее значение оценок вопросов проверки
19.1	Повторяется исполнение п.18.1	В соответствии с пунктом 18.1
19.2	Ознакомление с внутренними распорядительными требованиями по допуску персонала к КТ (да-1/частично - 0,2¸0,8/нет-0); Соблюдение инструкций по допуску персонала к КТ (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка)	Среднее значение оценок вопросов проверки
19.3	Повторяется исполнение п.1.1 для КТ	В соответствии с пунктом 1.1
19.4	Повторяется исполнение п.1.3	В соответствии с пунктом 1.3
19.5	Повторяется исполнение п.1.5	В соответствии с пунктом 1.5
19.6	Повторяется исполнение п.1.9	В соответствии с пунктом 1.9
19.7	Наличие расписок сотрудников о неразглашении КТ (да-1/нет-0) (Документальная проверка)	В соответствии с оценкой
19.8	Наличие утвержденной номенклатуры допущенных к КТ должностей (да-1/нет-0) (Документальная проверка)	В соответствии с оценкой
19.9	Повторяется исполнение п.1.1	В соответствии с пунктом 1.1
19.10	Повторяется исполнение п.1.2	В соответствии с пунктом 1.2
19.11	Повторяется исполнение 1.6 для личных дел	В соответствии с пунктом 1.6
19.12	Повторяется исполнение п.18.14	В соответствии с пунктом 18.14
20.1	Наличие положений устава и подразделений СБ (если они должны быть) (да-1/частично - 0,2¸0,8/нет-0); Ознакомление с уставом сотрудников (да-1/частично - 0,2¸0,8/нет-0); Соблюдение устава сотрудниками (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников, негласная проверка)	Среднее значение оценок вопросов проверки
20.2	Наличие должностных инструкций сотрудников (да-1/нет-0); Ознакомление сотрудников с должностными инструкциями (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников, негласная проверка)	Среднее значение оценок вопросов проверки
20.3	Наличие возможности организации физической охраны и физического сопровождения лиц (да-1/нет-0); Наличие сопроводительных документов (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников, негласная проверка)	Среднее значение оценок вопросов проверки
20.4	Наличие ответственного сотрудника за проведение ИВР (да-1/нет-0); Журнал учета ИВР (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников, негласная проверка)	Среднее значение оценок вопросов проверки
20.5	Имеется ли политика организации в отношении Пдн в соответствии с ФЗ-152 (да-1/нет-0) (Документальная проверка)	В соответствии с оценкой
20.6	Взаимодействие с правоохранительными органами и частными детективами по вопросам защиты ПдН (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка)	В соответствии с оценкой
20.7	Страхование сотрудников (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка)	В соответствии с оценкой
20.8	Наличие психологической службы (да-1/нет-0); Постоянный контроль психического состояния сотрудников (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка)	Среднее значение оценок вопросов проверки

20.9	Обеспечение ежегодной диспансеризации сотрудников (да/нет) (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка)	В соответствии с оценкой
20.10	Наличие общественных формирований (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка)	В соответствии с оценкой
21.1	Предусматриваются ли документально наличие общественных формирований (ОФ) (да-1/нет-0); Отсутствие ОФ из документально подтвержденных (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников)	Отсутствие ОФ-0. В остальных случаях среднее значение оценок вопросов проверки
21.2	Наличие документации о ОФ (да-1/частично - 0,2¸0,8/нет-0); Недовольство в коллективе по данному вопросу (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников)	Среднее значение оценок вопросов проверки
21.3	Повторяется исполнение п.21.2 для ИВР	В соответствии с пунктом 21.2
21.4	Повторяется исполнение п.21.2 для культурно-массовой работы	В соответствии с пунктом 21.2
21.5	Повторяется исполнение п.21.2 для спортивно-массовой работы	В соответствии с пунктом 21.2
21.6	Повторяется исполнение п.21.2 дополнительное материальное стимулирование сотрудников	В соответствии с пунктом 21.2
21.7	Повторяется исполнение п.21.2 для социальной защиты сотрудников, допущенных к КТ	В соответствии с пунктом 21.2
21.8	Наличие аналитических материалов анализа морально-психологического климата коллектива (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка)	В соответствии с оценкой
22.1	Наличие документации по обучению сотрудников (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка)	В соответствии с оценкой
22.2	Использование предусмотренных форм и методов обучения (да-1/частично - 0,2¸0,8/нет-0); Использование новых форм и методов обучения (да-1/нет-0) (Документальная проверка, опрос сотрудников)	Среднее значение оценок вопросов проверки
22.3	Наличие опросов и проверок сотрудников на квалификацию (да-1/частично - 0,2¸0,8/нет-0); Удовлетворяют ли знания сотрудников (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников)	Среднее значение оценок вопросов проверки
22.4	Наличие служебных проверок по фактам нарушений обращений с КТ (да-1/нет-0) (Документальная проверка)	В соответствии с оценкой
22.5	Наличие дополнительных занятий по календарному плану (да-1/частично - 0,2¸0,8/нет-0); Наличие дополнительных занятий (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников)	Среднее значение оценок вопросов проверки
23.1	Наличие документа, регламентирующего сбор информации ПДн сотрудников (да-1/нет-0); Ознакомление сотрудников с документом (да-1/частично - 0,2¸0,8/нет-0); Соблюдение сотрудниками регламента обращения с ПДн (да-1/нет-0) (Документальная проверка, опрос сотрудников, негласная проверка)	Среднее значение оценок вопросов проверки
23.2	Наличие обязательной информации по ПДн сотрудников (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка)	В соответствии с оценкой
23.3	Наличие документации по использованию ТС защиты ПДн сотрудников (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка)	В соответствии с оценкой
23.4	Наличие служебных проверок (если были инциденты) по фактам разглашения ПДн сотрудников (да-1/нет-0); Наличие сопроводительных документов служебных проверок (да-1/нет-0) (Документальная проверка)	Среднее значение оценок вопросов проверки

Приложение 5

Таблица П5 – Характер проверочных мероприятий и способ получения частных технических показателей оценки защищённости организационного канала утечки информации

№ частного показателя	Характер проверочных мероприятий, вопросы проверки (способы получения показателя)	Значение показателя M_{ij}
1	2	3
1.1	Наличие СЗЭД (если положено по нормативным документам) (да-1/нет); Наличие положения о СЗЭД (да-1/нет-0); Наличие ответственного лица за СЗЭД (да-1/нет-0); Наличие в СЗЭД правил аутентификации и идентификации (да-1/нет-0); Ведение протокола работы в СЗЭД (да-1/нет-0); Контроль по протоколам работы в СЗЭД (да-1/нет-0) (Обследование СЗЭД, контроль протоколов)	Если положено, но нет, или не работоспособна- 0. В остальных случаях среднее значение оценок вопросов проверки
1.2	Наличие положения о ЭЦП на предприятии (если ЭЦП имеется и должна быть) (да-1/нет-0); Наличие ответственного за функционирование ЭЦП (да-1/нет-0); Работоспособность ЭЦП (да-1/нет-0) (Обследование, контроль протоколов)	Если положено, но нет, - 0. В остальных случаях среднее значение
1.3	Наличие положения об автоматизированном контроле исполнения и движения документов (да-1/нет-0)	В соответствии с оценкой
1.4	Наличие помещений с обработкой и хранением носителей КТ, подлежащих оборудованию ОТС и СКУД (да-1/нет-0); Достаточность оснащенности ТСО (да-1/нет-0); Работоспособность ТСО (да-1/частично - 0,2¸0,8/нет-0); Наличие положения о размещении ТСО в помещениях (да-1/нет-0); Наличие протоколов и журналов работы ТСО (да-1/частично - 0,2¸0,8/нет-0); Достаточность оснащенности СКУД (да-1/нет-0); Работоспособность СКУД (да-1/частично - 0,2¸0,8/нет-0); Наличие положения о размещении СКУД (в помещениях (да-1/нет-0); Наличие протоколов и журналов работы СКУД (да-1/частично - 0,2¸0,8/нет-0) (Обследование, контроль протоколов)	Если нет СКУД или ОТС, или они не работоспособны- 0. В остальных случаях среднее значение оценок вопросов проверки
1.5	Наличие протоколов АРМ или журналов по сдаче под охрану помещений, посещения помещений (да-1/нет-0); Проведение контроля протоколов АРМ по сдаче под охрану помещений, посещения помещений уполномоченными лицами (да-1/частично - 0,2¸0,8/нет-0) (Обследование, контроль протоколов)	Если протоколы или журналы не ведутся- 0. В остальных случаях среднее значение оценок вопросов проверки
2.1	Наличие СКУД (если СКУД должна быть) (да-1/нет-0); Наличие положения о СКУД (да/нет); Наличие протоколов или журналов по осуществление контроля перемещения лиц в СКУД (да-1/нет-0); Наличие протоколов или журналов осуществление контроля перемещения сторонних сотрудников по протоколам работы СКУД (да-1/нет-0) (Обследование СКУД, контроль протоколов)	Если нет контроля перемещения лиц по СКУД- 0. В остальных случаях среднее значение оценок вопросов проверки
2.2	Наличие каналов связи с лицами, находящимися в служебных командировках (да-1/нет-0); Наличие положения о каналах связи с лицами находящимися в служебных командировках (да-1/нет-0); Наличие инструкции об осуществлении контроля лиц, находящихся в служебных командировках в служебное и не служебное время по каналам связи (да-1/нет-0) (Документальная проверка, опрос сотрудников)	Если нет связи - 0. В остальных случаях среднее значение оценок вопросов проверки
2.3	Наличие системы видеонаблюдения (СВН) (если она должна быть по нормативным документам) (Да-1/нет-0); Работоспособность СВН (да-1/нет-0); Наличие видеозаписей работы СВН (да-1/частично - 0,2¸0,8/нет-0); Наличие положения об осуществлении контроля за лицами находящихся на территории предприятия посредством СВН (да-1/нет-0) (Документальная проверка, обследования СВН)	Если нет СВН или она не работоспособна- 0. В остальных случаях среднее значение оценок вопросов проверки

3.1	Наличие поисковых технических средствах для выявления специальных ТС помещений (да-1/нет-0); Наличие положения об использовании поисковых технических средствах для выявления специальных ТС (да-1/нет-0); Наличие ответственного сотрудника со специальным образованием (да-1/нет-0); Работоспособность поисковых технических средств для выявления специальных ТС (да-1/нет-0) (Документальная проверка, опрос сотрудников, обследования ТС)	Если нет поисковых ТС или они не работоспособны- 0. В остальных случаях среднее значение оценок вопросов проверки
3.2	Наличие ТС обнаружения диктофонов, сотовых телефонов и видеокамер (да-1/нет-0); Наличие положения об использовании ТС обнаружения диктофонов, сотовых телефонов и видеокамер (да-1/нет-0); Наличие ответственного сотрудника со специальным образованием (да-1/нет-0); Работоспособность ТС обнаружения диктофонов, сотовых телефонов и видеокамер (да-1/нет-0) (Документальная проверка, опрос сотрудников, обследования ТС)	Если нет ТС или они не работоспособны- 0. В остальных случаях среднее значение оценок вопросов проверки
3.3	Наличие положения о размещении ТСЗИ в комнате проведения совещаний (да-1/нет-0); Наличие журналов/протоколов использования ТСЗИ в комнате проведения совещаний (да-1/частично - 0,2¸0,8/нет-0); Наличие ответственного сотрудника со специальным образованием (да-1/нет-0) Наличие инструкции об использовании ТСЗИ при проведении совещаний (да-1/нет-0); Работоспособность ТС обнаружения диктофонов, сотовых телефонов и видеокамер (да-1/нет-0) (Документальная проверка, опрос сотрудников, обследования ТСЗИ)	Если нет ТСЗИ или они не работоспособны- 0. В остальных случаях среднее значение оценок вопросов проверки
3.4	Наличие средств маскировки и пассивной защиты (да-1/нет-0); Фактическое использование средств маскировки и пассивной защиты (да-1/частично - 0,2¸0,8/нет-0); Наличие инструкции об использовании средств маскировки (да-1/нет-0) (Документальная проверка, обследования помещений)	Если нет средств маскировки и пассивной защиты или они не используются- 0. В остальных случаях среднее значение оценок вопросов проверки
3.5	Наличие ТСЗИ для средств звукоусилительной аппаратуры и др. технических средств обеспечения проведения совещания (да/нет); Работоспособность ТСЗИ для средств звукоусилительной аппаратуры и др. технических средств обеспечения проведения совещания (да-1/частично - 0,2¸0,8/нет-0); Наличие инструкции об санкционированное использовании звукоусилительной аппаратуры и др. технических средств обеспечения проведения совещания (да-1/нет-0) (Документальная проверка, обследования помещений)	Если нет средств ТСЗИ, ил они не исправны, а звукоусилительная аппаратура используется - 0. В остальных случаях среднее значение оценок вопросов проверки
3.6	Наличие положения о размещении СКУД при организации доступа на территорию объекта в помещения совещаний (да-1/нет-0); Наличие протоколов/журналов СКУД при организации доступа на территорию объекта в помещения совещаний (да-1/частично - 0,2¸0,8/нет-0); Работоспособность ТС СКУД (да-1/нет-0) (Документальная проверка, анализ протоколов СКУД, обследование помещений)	Если нет СКУД в помещениях проведения совещаний или они не исправны - 0. В остальных случаях среднее значение оценок вопросов проверки
3.7	Повторяется исполнение п.3.6 для средств видеонаблюдения - СВН	В соответствии с пунктом 3.6
4.1	Наличие технических средств досмотра багажа и личных вещей (если это предусмотрено нормативными документами) (да-1/нет-0); Наличие ответственного сотрудника со специальным образованием (да-1/нет-0); Фактическое использование технических средств для досмотра багажа и личных вещей (если это предусмотрено нормативными документами) (да-1/частично - 0,2¸0,8/нет-0); Наличие инструкции об использовании технических средств для досмотра багажа и личных вещей до и после приезда (да-1/нет-0) (Документальная проверка, опрос сотрудников, обследование досмотровых средств)	Если досмотровых ср-в нет (а должны быть) или фактически не используются - 0. В остальных случаях среднее значение оценок вопросов проверки
4.2	Повторяется исполнение п.2.2 для каналов связи	В соответствии с пунктом 4.2
4.3	Повторяется исполнение п.2.2 для контроля местонахождения сотрудника	В соответствии с пунктом 4.2

4.4	Наличие положения (инструкции по применению) полиграфа (да-1/нет-0); Наличие сотрудника со специальным образованием (да-1/нет-0); Фактическое использование полиграфа (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников, обследование ТС)	Если нет полиграфа (а должен быть), или он не исправен или фактически не используется - 0. В остальных случаях среднее значение оценок вопросов проверки
4.5	Наличие средств видеофиксации при сопровождении (если это требуется) (гласных ил негласных) (да-1/нет-0); Наличие инструкции по использованию средств видеофиксации (гласных/негласных) (да-1/нет-0); Использование (гласное и негласное по возможности и необходимости) средств видеофиксации при сопровождении (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников, обследование ТС)	Если нет технических средств (а должны быть), они не исправны или фактически не используются - 0. В остальных случаях среднее значение оценок вопросов проверки
5.1	Повторяется исполнение п.1.1 для корпоративной ЛВС	В соответствии с пунктом 1.1
5.2	Повторяется исполнение п.1.2 для корпоративной ЛВС	В соответствии с пунктом 1.2
5.3	Используется ли выход в глобальные информационные сети (нет-1/используется через сетевой экран с распределением доступа к ИР -0,9 / через сетевой экран без распределения доступа -0,2/свободный выход-0); Используется ли выход в корпоративные информационные сети (нет-1/используется через сетевой экран с распределением доступа к ИР -0,9 / через сетевой экран без распределения доступа-0,2 /свободный выход-0); Используется ли беспроводные сегменты корпоративных информационных сетей (нет-1/используются с защитой WPA-WPA2-0,95/используются без защиты-0); Используется ли антивирусное ПО (нет -0/не достаточно используется-0,3/ не используется-0); Постоянно ли обновляются базы антивирусного ПО (не обновляются-0/ частично обновляются - 0,2¸0,8/обновляются своевременно-1); Телекоммуникации смонтированы «скрытым способом» (нет свободного доступа посторонних лиц) (да-1/частично - 0,2¸0,8/нет-0); Телекоммуникации проходят только через помещения, контролируемые предприятием (организацией), т.е. «охраняемые помещения» (да-1/нет-0); Организован контроль доступа к ИР с процедурами аутентификации и идентификации на основе сертифицированных специализированных СЗИ (да-1/частично - 0,2¸0,8/нет-0); Осуществляется ли аудит ИБ (да-1/частично - 0,2¸0,8/нет-0); Имеются ли замечания и предложения по итогам аудита ИБ (нет-0/не значительные0,3/да-0,6); Соблюдается ли периодичность проведения аудита ИБ (да-1/нет-0); Существует ли должность администратора безопасности корпоративной ЛВС (да-1/нет-0); Утверждена ли политика ИБ на предприятии (да-1/нет-0); Выполняются ли основные положения политики ИБ на предприятии (при ее наличии) (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников, контроль протоколов, обследование сегмента ЛВС)	Если имеется свободный выход в глобальные или корпоративные сети, не используется или не обновляется антивирусное ПО, не проводится аудит ИБ, нет политики безопасности ИБ (а она должна быть по требованиям) - 0. В остальных случаях среднее значение оценок вопросов проверки
5.4	Повторяется исполнение п.1.4	В соответствии с пунктом 1.4
5.5	Наличие специализированного ПО анализа информации (по тематике близкой к КТ предприятия) из существующих открытых источников (да-1/нет-0); Использование специализированного ПО анализа информации (по тематике близкой к КТ предприятия) из существующих открытых источников (да-1/частично - 0,2¸0,8/нет-0) (Опрос сотрудников, обследование специализированного ПО)	Если нет ПО анализа информации (по тематике близкой к КТ предприятия) - 0. В остальных случаях среднее значение
6.1	Повторяется исполнение п.2.1 для контроля нахождение иностранных представителей	В соответствии с пунктом 2.1
6.2	Повторяется исполнение п.1.1 для КВС (корпоративной вычислительной сети) организации	В соответствии с пунктом 1.1
6.3	Наличие технических ограничений, протоколов, контактов с иностранными партнерами сотрудников (да-1/частично - 0,2¸0,8/нет-0) (Опрос сотрудников, контроль протоколов, обследование ТС)	В соответствии с оценкой

6.4	Исключение возможности электронных контактов с зарубежными партнерами с СВТ на территории организации (да-1/частично - 0,2¸0,8/нет-0) (Опрос сотрудников, контроль протоколов, обследование ТС)	В соответствии с оценкой
6.5	Повторяется исполнение п.1.2 для контактов с иностранными партнерами сотрудников	В соответствии с пунктом 1.2
7.1	Наличие специализированых помещений с проведением работ по НИР и ОКР (да-1/нет-0); Наличие положения о помещениях с проведением работ по НИР и ОКР (да-1/нет-0); Наличие в помещении ТСО (да-1/частично - 0,2¸0,8/нет-0); Наличие протоколов/журналов работы ТСО (да-1/частично - 0,2¸0,8/нет-0); Наличие в помещении СКУД (да-1/нет-0); Наличие протоколов/журналов работы СКУД (да-1/частично - 0,2¸0,8/нет-0) Наличие в помещении СВН (да-1/нет-0); Работоспособность ТСО (да-1/частично - 0,2¸0,8/нет-0); Работоспособность СКУД (да-1/частично - 0,2¸0,8/нет-0); Работоспособность СВН (да-1/частично - 0,2¸0,8/нет-0); (Документальная проверка, опрос сотрудников, контроль протоколов, обследование ОТС, СКУД и СВН помещений)	Если нет ТСО, СКУД, если они не работоспособны - 0. В остальных случаях среднее значение оценок вопросов проверки
7.2	Наличие противокражных систем для контроля и учета перемещения и выноса образцов, носителей КТ (если они должны быть) (да-1/нет-0); Наличие инструкции об использовании противокражных систем для контроля и учета перемещения и выноса образцов, носителей КТ (да-1/нет-0); Наличие ответственного сотрудника со специальным образованием (да-1/нет-0); Фактическое использование противокражных систем для контроля и учета перемещения между помещениями и выноса из помещений образцов, носителей КТ (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников, контроль протоколов, обследование ОТС, СКУД и СВН помещений)	Если нет противокражных систем для контроля и учета перемещения и выноса образцов, носителей КТ или они не используются - 0. В остальных случаях среднее значение
8.1	Повторяется исполнение п.7.1	В соответствии с пунктом 7.1
8.2	Повторяется исполнение п.1.2 для каналов электронной связи с инспекторскими и надзорными органами.	В соответствии с пунктом 1.2
9.1	Повторяется исполнение п. 7.1 для средств КПиОР	В соответствии с пунктом 7.1
9.2	Соответствие требованиям нормативных документов по классам защиты технического укрепления элементов строительных конструкций периметры ограждений территорий, КПП (да-1/частично - 0,2¸0,8/нет-0) (Обследование технического укрепления)	В соответствии с оценкой
10.1	Повторяется исполнение п.7.1 для средств КПиОР	В соответствии с пунктом 7.1
10.2	Соответствие требованиям нормативных документов по классам защиты технического укрепления элементов строительных конструкций защищаемые помещения с хранением носителей КТ (да-1/частично - 0,2¸0,8/нет-0) (Обследование технического укрепления)	В соответствии с оценкой
11.1	Наличие СКУД (д-1/нет-0); Работоспособность СКУД (да-1/частично - 0,2¸0,8/нет-0); Наличие протоколов/журналов СКУД (да-1/частично - 0,2¸0,8/нет-0); Наличие ответственного сотрудника за СКУД (да-1/нет-0); Поддержание полноты и актуальности БД (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников, контроль протоколов, обследование СКУД)	Если нет технических средств (а они должны быть) или они не работоспособны- 0. В остальных случаях среднее значение
12.1	Повторяется исполнение п.11.1 для средств ОТС	В соответствии с пунктом 11.1
13.1	Наличие протоколов (журналов) передачи данных по закрытым каналам (да-1/нет-0); Контроль протоколов (журналов) передачи данных по закрытым каналам на предмет выявления несанкционированных действий (да-1/частично - 0,2¸0,8/нет-0) (контроль протоколов)	Если нет протоколов (журналов)- 0. В остальных случаях среднее значение
13.2	Наличие протоколов (журналов) передачи данных по закрытым каналам (да-1/нет-0); Контроль протоколов (журналов) на предмет возможности и выявления НСД к информационным ресурсам закрытых каналов (да-1/частично - 0,2¸0,8/нет-0) (контроль протоколов)	Если нет протоколов (журналов)- 0. В остальных случаях среднее значение

13.3	Наличие журналов (протоколов) информационного обмена (да-1/нет-0); Контроль ведения установленных журналов (протоколов) информационного обмена (да-1/частично - 0,2¸0,8/нет-0) (контроль протоколов)	Если нет протоколов (журналов)- 0. В остальных случаях среднее значение
14.1	Наличие журналов (протоколов) функционирования ТСЗИ (да-1/нет-0) (контроль протоколов)	В соответствии с оценкой
14.2	Работоспособность функционирования ТСЗИ (да-1/нет-0) (обследование ТСЗИ)	В соответствии с оценкой
14.3	Наличие специальных технических средств поиска и обнаружения закладных устройств (да-1/нет-0); Наличие инструкций по применению специальных технических средствах поиска и обнаружения закладных устройств (да-1/нет-0); Наличие ответственного сотрудника со специальным образованием (да-1/нет-0); Работоспособность специальных технических средств поиска и обнаружения закладных устройств (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников, контроль протоколов, обследование)	Если нет технических средств или они не работоспособны- 0. В остальных случаях среднее значение
15.1	Наличие технических средств (способов) уничтожения носителей КТ, образцов, черновиков и т.д. (да-1/нет-0); Наличие инструкции о технических средствах (способах) уничтожения носителей КИ, образцов, черновиков и т.д. (да-1/нет-0) (Документальная проверка, опрос сотрудников, обследование)	Если нет технических средств или они не работоспособны- 0. В остальных случаях среднее значение
15.2	Наличие технических возможностей должной утилизации носителей КТ (да-1/нет-0)	В соответствии с оценкой
16.1	Наличие технических средств (способов) уничтожения образцов, черновиков, брака (да-1/нет-0); Наличие технических возможностей должной утилизации производственного брака (да-1/частично - 0,2¸0,8/нет-0) (Опрос сотрудников, обследование)	Среднее значение оценок вопросов проверки
17.1	Наличие средств маскировки, пломбирования и опечатывания (да-1/частично - 0,2¸0,8/нет-0); Наличие инструкций о применении средств маскировки, пломбирования и опечатывания (да-1/нет-0); Фактическое использование средств маскировки, пломбирования и опечатывания (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, опрос сотрудников, обследование)	Если нет технических средств или они не работоспособны или фактически не используются- 0. В остальных случаях среднее значение
17.2	Повторяется исполнение п.7.2 для контроля и учета сохранности продукции	В соответствии с пунктом 7.2
18.1	Наличие помещений с обработкой и хранением личных дел сотрудников (да-1/нет-0); Наличие в данных помещениях ТСО (да-1/нет-0); Работоспособность ТСО (да-1/частично - 0,2¸0,8/нет-0); Наличие протоколов/журналов работы ТСО для данных помещений (да-1/частично - 0,2¸0,8/нет-0); Наличие СКУД для данных помещений (да-1/нет-0); Работоспособность СКУД (да-1/частично - 0,2¸0,8/нет-0); Наличие протоколов/журналов работы СКУД для данных помещений (да-1/нет-0) (Документальная проверка, контроль протоколов, обследование ОТС и СКУД)	Если нет технических средств или они не работоспособны или фактически не используются- 0. В остальных случаях среднее значение
18.2	Контроль по протоколам АРМ по сдаче под охрану помещений, посещения помещений уполномоченными лицами с обработкой и хранением личных дел сотрудников (да-1/частично - 0,2¸0,8/нет-0) (Контроль протоколов)	В соответствии с оценкой
19.1	Повторяется исполнение п.18.1 для помещений с персональными данными сотрудников	В соответствии с пунктом 18.1
19.2	Повторяется исполнение п.18.2 для помещений с персональными данными сотрудников	В соответствии с пунктом 18.2
20.1	Контроль лиц, в служебное и не служебное время по служебным каналам связи (при согласии и необходимости) (да-1/частично - 0,2¸0,8/нет-0) (Опрос сотрудников, контроль протоколов)	В соответствии с оценкой
20.2	Контроль лиц, в служебное и не служебное время по их местоположению (GPS и т.д.) (при согласии и необходимости) (да-1/частично - 0,2¸0,8/нет-0) (Опрос сотрудников, контроль протоколов)	В соответствии с оценкой
20.3	Повторяется исполнение п.4.4	В соответствии с пунктом 4.4
20.4	Наличие средств аудио и видеофиксации (да-1/нет-0); Использование (гласное и негласное) средств аудио и видеофиксации (да-1/нет-0) (Опрос сотрудников, контроль протоколов)	Среднее значение оценок вопросов проверки

21.1	Наличие сотрудника со специальным образованием (да-1/нет); Наличие комплексов для психологического тестирования сотрудников (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, обследование, опрос сотрудников)	Среднее значение оценок вопросов проверки
21.2	Повторяется исполнение п.4.4	В соответствии с пунктом 4.4
22.1	Наличие тестов для тестирования знаний сотрудников (да-1/частично - 0,2¸0,8/нет-0); Проведение тестирований знаний сотрудников (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, обследование, опрос сотрудников)	Среднее значение оценок вопросов проверки
23.1	Периодическое проведение аудита политики ИБ (да-1/нет-0); Соответствие технических средств обработки ПдН требованиям нормативных документов (при необходимости) (да-1/частично - 0,2¸0,8/нет-0) (Документальная проверка, обследование, опрос сотрудников)	Среднее значение оценок вопросов проверки

Литература

1. Аверченков В. И., Рытов М. Ю. Организационная защита информации: учебное пособие для вузов. – М.: Флинта, 2011. – 184 с.

2. Глобальное исследование утечек конфиденциальной информации в I полугодии 2018 года // Аналитический центр InfoWatch [Электронный ресурс].2019. – URL: http://itzashita.ru/wp-content/uploads/2018/10/infowatch_global_report_2018_half_year.pdf (дата обращения: 05.05.2019).

3. Основные внутренние угрозы информационной безопасности 2019 // Аналитический центр Anti-Malware.ru [Электронный ресурс]. 2019. – URL: https://www.anti-malware.ru/analytics/Market_Analysis/key-infosecurity-business-trends (дата обращения: 05.05.2019).

4. Морозов А. В., Полякова Т. А. Организационно-правовое обеспечение информационной безопасности. Монография. – М.: РПА Минюста России, 2013. – 276 с.

5. Ищейнов В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации: учебное пособие для вузов. 2-е изд. – М.: Форум, 2014. – 255 с.

6. Хорев А. А. Организация защиты конфиденциальной информации в коммерческой структуре // Защита информации. Инсайд. 2015. № 1 (61). С. 14-17.

7. Хорев А. А. Организация защиты конфиденциальной информации в коммерческой структуре // Защита информации. Инсайд. 2015. № 2 (62). С. 14-25.

8. Хорев А. А. Проблемные вопросы защиты информации, отнесенной к профессиональной тайне // REDS: Телекоммуникационные устройства и системы. 2017. Т. 7. № 4. С. 504-506.

9. James F. Broderp. Risk analysis and the security survey. – Butterworth-Heinemann Publ., 2006. – 393 p.

10. Charles A. Sennewald, Curtis Baillie. Effective Security Management. – Butterworth-Heinemann Publ., 2015. – 402 p.

11. Тельный А. В., Монахов М. Ю. Динамическая модель достаточности инженерно-технического укрепления элементов строительных конструкций

территорий, зданий и помещений объектов для предотвращения несанкционированного доступа // Динамика сложных систем – XXI век. 2016. № 1. С. 41-48.

12. Тельный А. В., Монахов Ю. М., Монахов М. Ю. Оценка защищенности информационных ресурсов организации от несанкционированного доступа нарушителей в здания и помещения // Известия высших учебных заведений. Технология текстильной промышленности. 2016. № 5. С. 259-263.

13. Тельный А. В., Монахов М. Ю., Романова А. Г., Яковлева Е. И. О методике оценки защищенности организационного канала утечки информации на предприятии // Вестник Адыгейского государственного университета. Серия 4: естественно-математические и технические науки. 2019. № 1. С. 141-145.

14. Хиценко В. Е. Математическая статистика для мониторинга информационной безопасности. Непараметрические методы статистики в примерах и задачах. Монография. – Saarbrücken: LAP Lambert Academic Publishing, 2013. – 212 с.

References

1. Averchenkov V. I., Rytov M. Yu. *Organizacionnaya zashchita informacii: uchebnoe posobie dlya vuzov.* [Organizational Information Security]. Moscow, Flinta Publ., 2011. 184 p. (in Russian).

2. Globalnoe issledovanie utechek konfidencialnoy informacii v I polugodii 2018 goda [Global study of confidential information leaks in the first half of 2018]. *Analiticheskiy centr InfoWatch* [Analytical center InfoWatch], 05 May 2019. Available at: http://itzashita.ru/wp-content/uploads/2018/10/infowatch_global_report_2018_half_year.pdf (accessed 05 May 2019) (in Russian).

3. Osnovnye vnutrennie ugrozy informacionnoy bezopasnosti 2019 [The main internal threats to information security 2019]. *Analiticheskiy centr Anti-Malware.ru* [Analytical center Anti-Malware.ru], 05 May 2019. Available at: https://www.anti-malware.ru/analytics/Market_Analysis/key-infosecurity-business-trends (accessed 05 May 2019) (in Russian).

4. Morozov A. V., Polyakova T. A. *Organizacionno-pravovoe obespechenie informacionnoj bezopasnosti. Monografiya.* [Organizational and legal support of information security. Monograph]. Moscow, Russian law Academy of the Ministry of justice of the Russian Federation Publ., 2013. 276 p. (in Russian).

5. Ishchejnov V. Ya. *Organizacionnoe i tekhnicheskoe obespechenie informacionnoj bezopasnosti. Zashchita konfidencial'noj informacii: uchebnoe posobie dlya vuzov*. [Organizational and technical information security. Protection of confidential information]. Moscow, Forum Publ., 2014. 255 p. (in Russian).

6. Horev A. A. Organization of confidential information protection in a commercial structure. *Zasita informacii. Inside*, 2015, vol. 61, no. 1, pp. 14-17 (in Russian).

7. Horev A. A. Organization of confidential information protection in a commercial structure. *Zasita informacii. Inside*, 2015, vol. 62, no. 2, pp. 14-25 (in Russian).

8. Horev A. A. Problem issues of protection of information classified as professional secrets. *REDS: Telecommunication devices and systems*, 2017, vol. 7, no. 4, pp. 504-506 (in Russian).

9. James F. Broderp. Risk analysis and the security survey. – Butterworth-Heinemann Publ., 2006. – 393 p.

10. Charles A. Sennewald, Curtis Baillie. Effective Security Management. – Butterworth-Heinemann Publ., 2015. – 402 p.

11. Telny A. V., Monakhov M. Yu. Dynamic model of adequacy of engineering and technical strengthening of elements of building structures of territories, buildings and premises of objects to prevent unauthorized access. *Dynamics of Complex Systems – XXI century*, 2016, no. 1, pp. 41-48 (in Russian).

12. Telny A. V., Monakhov Yu. M., Monakhov M. Yu. Evaluation of the security of information resources of the organization from unauthorized access of violators to buildings and premises. *News of higher educational institutions. Technology of the textile industry*, 2016, vol. 365, no. 5, pp. 259-262 (in Russian).

13. Telny A. V., Monakhov M. Yu. Romanova A. G., Yakovleva E. I. About the method of assessment of security of the organizational channel of information leakage at the enterprise. *The Bulletin of the Adyghe State University. Series "Natural-Mathematical and Technical Sciences"*, 2019, no. 1, pp.141-145 (in Russian).

14. Hicenko V. E. *Matematicheskaya statistika dlya monitoringa informacionnoy bezopasnosti. Neparametricheskie metody statistiki v primerah i zadachah. Monografiya.* [Mathematical statistics for information security monitoring. Nonparametric methods of statistics in examples and problems. Monograph]. Saarbrücken, LAP Lambert Academic Publishing, 2013. 212 p. (in Russian).

Статья поступила 14 июня 2019 г.

Информация об авторах

Тельный Андрей Викторович – кандидат технических наук, доцент. Доцент кафедры информатики и защиты информации. Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых. Область научных интересов: информационная безопасность; радиотехнические средства позиционирования подвижных объектов; технические средства защиты от несанкционированного доступа. E–mail: andre.izi@mail.ru.

Яковлева Екатерина Игоревна – студент-исследователь кафедры информатики и защиты информации. Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых. Область научных интересов: информационная безопасность; технические средства защиты информации. E–mail: katerina_yakov@bk.ru.

Романова Алина Георгиевна – студент-исследователь кафедры информатики и защиты информации. Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых. Область научных интересов: информационная безопасность; технические средства защиты информации. E–mail: romanova.ailna@mail.ru.

Адрес: 600000, Россия, г. Владимир, ул. Горького, д. 87.

Audit of security of the organizational channel of information leakage which is the trade secret of the organization

A. V. Telny, E. I. Iakovleva, A. G. Romanova

Problem statement. *The development of modern information technologies, information and data transmission means entails an increase of the importance information protection which is a trade secret of the organization. Leakage of information which is a trade secret of the organization occurs mainly through the organizational channel. The protection state of such channel must be constantly monitored and controlled.* ***The purpose of the paper*** *is to develop a method for assessing the security of the organizational channel of information leakage of trade secrets of the organization. This method can be used to automate the control of compliance with the requirements of normative documents in the field of information security, the assessment of the level of executive employee discipline and knowledge and skills test in the field of information security of the object personnel.* ***Methods***. *Standard methods of system analysis, morphological analysis and expert evaluations were used to analyze the security of organizational channel of information leakage.* ***Novelty***. *The novelty of the presented solution lies in sources of information leakage standard lists creation and causes of information leakage, organizational and technical protective mechanisms, evaluation criteria for individual and group indicators of security of the organizational channel of information leakage.* ***Results***. *The technique of audit the security of the organizational channel of secret information leakage is formed.* ***Practical relevance***. *The developed method can be implemented as a making decisions support system to audit the security of the organizational channel of leakage to protect the information, representing a trade secret of the organization.*

Key words: *information security, disclosure of information, information leakage through the organizational channel, security audit of the organizational channel, trade secret of the organization.*

Information about Authors

Andrey Viktorovich Telny – Ph.D. of Engineering Sciences. Associate Professor at the Department of Informatics and Information Security. Vladimir State University named after Alexander Grigorievich and Nikolai Grigorievich Stoletovs. Field of research: information security; radio technical means of positioning moving objects; technical means of protection against unauthorized access. E-mail: andre.izi@mail.ru.

Ekaterina Igorevna Iakovleva – research-student of the Department at the Department of Informatics and Information Security. Vladimir State University named after Alexander Grigorievich and Nikolai Grigorievich Stoletovs. Field of research: information security; technical means of information protection. E-mail: katerina_yakov@bk.ru.

Alina Georgievna Romanova – research-student of the Department at the Department of Informatics and Information Security. Vladimir State University named after Alexander Grigorievich and Nikolai Grigorievich Stoletovs. Field of research: information security; technical means of information protection. E-mail: romanova.ailna@mail.ru.

Address: Russia, 600000, Vladimir, Gorky str., 87.