

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 10.05.03 –

Информационная безопасность
автоматизированных систем

Специализация -

Защищенные автоматизированные
системы управления

ДИПЛОМНЫЙ ПРОЕКТ

на тему

МЕТОДИКА ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТА

Студент



Шантаев Алексей Юрьевич

Руководитель



Зефилов С.Л.

Нормоконтролёр



Фатеев А.Г.

Рецензент



В.Д. Юрлов

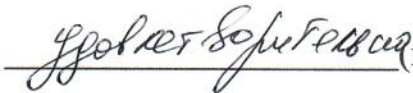
Работа допущена к защите (протокол заседания кафедры от 15.06.2020 № 12)

Заведующий кафедрой



С.Л. Зефилов

Работа защищена с отметкой
от 26.06.2020 № 20



(протокол заседания ГЭК

Секретарь ГЭК



А.П. Иванов

Пенза 2020

Оглавление

Введение	4
1 Разработка способа оценки текущего уровня ИБ	5
1.1 Разработка модели оценки текущего уровня ИБ.....	5
1.2 Требования ИБ для областей обеспечения ИБ	6
1.3 Разработка и описание способа оценки текущего уровня ИБ на основе оценки соответствия защитных мер объекта требованиям к ИБ объекта	7
1.4 Оценка текущего уровня информационной безопасности объекта	8
1.5 Определение текущего уровня информационной безопасности объекта.....	14
2 Разработка способа оценки развития уровня ИБ	15
2.1 Разработка модели оценки развития уровня ИБ.....	15
2.2 Требования к процессам управления информационной безопасностью	17
2.3 Разработка и описание способа оценки возможности процессов управления информационной безопасностью	17
2.3.1 Формирование структуры уровней возможности процессов и производных показателей возможности процессов для каждого уровня. ...	17
2.3.2 Разработка основных показателей возможности процессов.	19
2.3.3 Разработка способа измерения основных показателей возможности процессов.....	21
2.3.4 Разработка способа формирования оценки возможности процессов..	23
2.3.5 Формирование итоговой оценки возможности процессов.	24
3 Формирование итоговой оценки уровня ИБ объекта.....	25
4 Разработка и описание методики оценки ИБ объекта.....	26
5 Вредные психофизиологические факторы, влияющие на	27

психоэмоциональное состояние специалиста по защите информации. Методы и	27
средства физической культуры, снижающие их воздействие	27
5.1 Вредные психофизиологические факторы, влияющие на психоэмоциональное состояние специалиста по защите информации	27
5.2 Методы и средства физической культуры, снижающие воздействие вредных психофизиологических факторов	31
Заключение	33
Список использованных источников	34
Приложение А.....	35
А.1 Требования по обеспечению защиты информации при управлении доступом.....	35
А.2 Требования по обеспечению защиты информации при защите от вредоносного кода.....	37
А.3 Требования по обеспечению защиты информации при дистанционном режиме	39
А.4 Требования по обеспечению защиты информации информационной инфраструктуры	40
Приложение Б	41
Приложение В.....	56
В.1 Идентификация и определение ценности активов.....	56
В.2 Идентификация и оценка угроз ИБ	56
В.3 Идентификация и оценка уязвимостей активов	58
В.4 Анализ рисков ИБ.....	58
В.5 Оценивание рисков ИБ	59
В.6 Обработка рисков ИБ	60
Приложение Г	62

Введение

Организации, бизнес которых во многом зависит от информационной сферы, для достижения целей бизнеса должны поддерживать информационную безопасность на необходимом уровне.

Совершенствование, улучшение информационной безопасности (ИБ) возможно при условии знания состояний характеристик и параметров используемых защитных мер, процессов управления и понимания степени их соответствия требуемым результатам. Понять это можно только по результатам оценки ИБ организации, полученной с помощью модели оценки ИБ на основании свидетельств оценки и критериев оценки.

Критерии оценки — это все то, что позволяет установить значения оценки для объекта оценки. В качестве критериев оценки ИБ могут использоваться требования ИБ, процедуры ИБ, сочетание требований и процедур ИБ.

Оценка ИБ осуществляется с помощью внешнего или внутреннего аудита ИБ. Оценка ИБ заключается в выработке оценочного суждения относительно возможности (зрелости) процессов управления ИБ, адекватности защитных мер на основе измерения и оценивания критических элементов (факторов) объекта оценки. Проводится оценка с использованием методики оценки, в основе которой лежат способы оценки измеряемых элементов объекта оценки. Часто методики оценки при проведении аудита ИБ направлены или на оценку соответствия применяемых защитных мер, или на оценку процессов управления ИБ.

В работе предлагается методика оценки ИБ, включающая оценку соответствия защитных мер и оценку возможности процессов управления ИБ. Целью разработки методики оценки информационной безопасности объекта является определение способов оценки текущего уровня ИБ, оценки развития уровня ИБ и способа итоговой оценки ИБ объекта.

1 Разработка способа оценки текущего уровня ИБ

1.1 Разработка модели оценки текущего уровня ИБ

Целью оценки текущего уровня ИБ является определение степени соответствия защитных мер объекта установленным требованиям ИБ, являющимся критерием оценки.

Для проведения оценки необходимо:

- определить показатели, позволяющие оценить выполнение требований;
- определить способы измерения показателей (измерение основных мер);
- определить способы вычисления оценок показателей (вычисление производных мер);
- определить способ формирования итоговой оценки текущего уровня ИБ.

На рисунке 1 представлена модель оценки текущего уровня ИБ.

В модели показано, что:

- оцениваемые области обеспечения ИБ описываются совокупностью основных показателей, для которых должны быть известны и применимы способы измерения;
- способы измерения основных показателей дают возможность получить оценки основных показателей;
- каждая оцениваемая область обеспечения ИБ обозначается производным показателем, для которых должны быть определены способы вычисления оценок производных показателей;
- способы вычисления оценок производных показателей дают возможность получить оценки производных показателей;
- совокупность оценок производных показателей являются основой для формирования итоговой оценки текущего уровня ИБ.

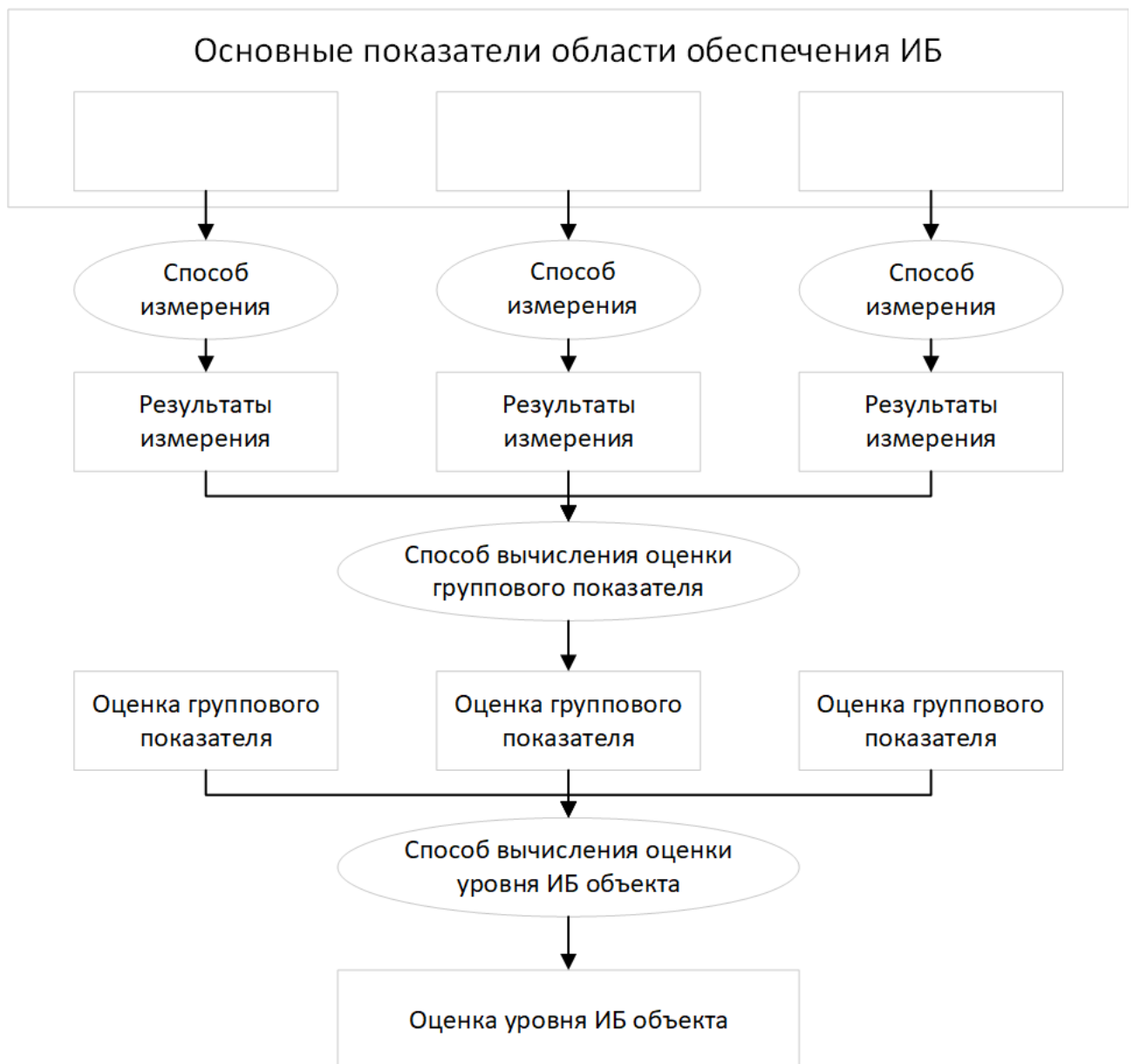


Рисунок 1 – Модель оценки текущего уровня ИБ

1.2 Требования ИБ для областей обеспечения ИБ

Для оценки ИБ выбраны следующие области обеспечения ИБ:

- защита информации при управлении доступом;
- защита информации от вредоносного кода;
- защита информации при дистанционном режиме;
- защита информационной инфраструктуры.

Требования ИБ для указанных областей обеспечения ИБ представлены в Приложении А.

1.3 Разработка и описание способа оценки текущего уровня ИБ на основе оценки соответствия защитных мер объекта требованиям к ИБ объекта

Для оценки соответствия ИБ объекта установленным требованиям используются производные и основные показатели ИБ. Производные показатели ИБ отражают области обеспечения ИБ. Основные показатели отражают требования ИБ, предъявляемые в областях обеспечения ИБ. Оценки производных показателей ИБ определяют оценки областей обеспечения ИБ. Оценки основных показателей ИБ определяют оценки выполнения установленных требований.

Оценка основных показателей ИБ осуществляются с помощью анкет, каждая из которых содержит производный показатель ИБ и входящие в него основные показатели ИБ, шкалу для оценивания основных показателей.

Все основные показатели должны быть оценены. Оценка основного показателя формируется с помощью экспертного оценивания и определяет степень выполнения требований. Устанавливается следующая шкала степени выполнения требований:

- «нет» – оценке присваивается значение, равное нулю;
- «частично» – оценке присваивается значение 0,25, 0,5 или 0,75;
- «да» – оценке присваивается значение, равное единице.

Оценка основного показателя ИБ основывается на свидетельствах аудита, в качестве основных источников которых используются:

- внутренние нормативные документы проверяемой организации и, при необходимости, документы третьих лиц, относящиеся к обеспечению ИБ;
- устные высказывания сотрудников проверяемой организации в процессе проводимых опросов;
- результаты наблюдений членов аудиторской группы за деятельностью сотрудников проверяемой организации в области ИБ.

Оценка основного показателя ИБ определяется с помощью экспертного оценивания. Проводится анализ нормативных, распорядительных и других

документов, имеющих отношение к проверяемым областям ИБ, и уточняется информация с помощью опросов сотрудников и наблюдения за деятельностью.

Шкала для оценивания основных показателей формируется на основании следующих критериев.

Если в результате оценивания основного показателя делается вывод о невыполнении соответствующих требований ИБ, то оценке основного показателя присваивается значение, равное нулю.

Если в результате оценивания основного показателя делается вывод о частичном выполнении соответствующих требований ИБ, то оценка основного показателя может быть установлена равной 0,25, 0,5 или 0,75 (в зависимости от степени выполнения требований ИБ).

Если в результате оценивания основного показателя делается вывод о полном выполнении соответствующих требований ИБ, то оценке основного показателя присваивается значение, равное единице.

Оценка производного показателя (O_{Pi}) вычисляется из оценок основных показателей (O_{Pij}) следующим образом:

$$O_{Pi} = \sum_j \alpha_{ij} \times O_{Pij},$$

где:

- α_{ij} – коэффициент значимости, определяющий важность основного показателя;
- i – номер производного показателя;
- j – номер основного показателя.

Итоговая оценка LT текущего уровня ИБ определяется по наименьшему значению из оценок производных показателей областей обеспечения ИБ:

$$LT = \min_i Pi$$

1.4 Оценка текущего уровня информационной безопасности объекта

Текущий уровень ИБ объекта определяется с помощью производных и основных показателей ИБ, позволяющих оценить степень выполнения

установленных требований ИБ. Для разработки способа оценки использовались выбранные области обеспечения ИБ:

- защита информации при управлении доступом;
- защита информации от вредоносного кода;
- защита информации при дистанционном режиме;
- защита информационной инфраструктуры.

Таблица 1 – Обозначение и наименование производных показателей ИБ

Обозначение производного показателя ИБ	Наименование производного показателя ИБ
P1	Защита информации при управлении доступом
P2	Защита информации от вредоносного кода
P3	Защита информации при дистанционном режиме
P4	Защита информационной инфраструктуры

Основные показатели ИБ и анкеты для их оценки приведены в Приложении Б. Приложение содержит формы, каждая из которых содержит производный показатель ИБ и входящие в него основные показатели ИБ, шкалу для оценивания основных показателей и коэффициенты значимости каждого основного показателя.

Коэффициенты значимости основных показателей определены экспертами. В определении коэффициентов значимости участвовали 4 эксперта. Для оценивания коэффициентов значимости применялся метод балльного оценивания при использовании десятибалльной шкалы.

Каждый эксперт выставляет балльные оценки b_{ij}^k (k -количество экспертов) основным показателям, соответствующие их значимости. На основании балльных оценок, выставленных k -экспертом, вычисляются оценки коэффициентов значимости для каждого основного показателя следующим образом

$$\alpha_{ij}^k = \frac{b_{ij}^k}{\sum_{j=1}^{m_i} b_{ij}^k},$$

где m_i – количество основных показателей у i -ого производного показателя.

При этом должно выполняться условия нормировки:

$$\sum_{j=1}^{m_i} \alpha_{ij}^k = 1$$

Групповая оценка экспертов коэффициентов значимости для каждого основного показателя вычисляется как среднее арифметическое индивидуальных оценок экспертов коэффициентов значимости следующим образом:

$$\alpha_{ij} = \frac{\sum_{j=1}^{m_i} \alpha_{ij}^k}{k}$$

При этом должно выполняться условия нормировки:

$$\sum_{j=1}^{m_i} \alpha_{ij} = 1$$

Для проведения оценки коэффициентов значимости основных показателей производного показателя Р1 «Защита информации при управлении доступом» экспертам представлено множество основных показателей Р1.1 – Р1.13. Результаты таковы.

Таблица 2 – Балльные оценки коэффициентов значимости основных показателей, выставленные экспертами

Э ОП	Р1.	Р1.	Р1.	Р1.4	Р1.	Р1.	Р1.	Р1.8	Р1.9	Р1.10	Р1.11	Р1.12	Р1.13
Эксперт1	8	8	9	6	7	6	7	7	7	6	8	7	6
Эксперт2	9	9	9	8	7	7	9	9	8	8	7	6	6
Эксперт3	7	8	8	7	9	8	7	8	6	6	7	7	8
Эксперт4	9	9	7	6	7	6	6	6	7	7	8	8	7

Таблица 3 – Оценки коэффициентов значимости для каждого основного показателя, вычисленные на основании балльных оценок коэффициентов значимости основных показателей, выставленных экспертами

Э ОП	P1.1	P1.2	P1.3	P1.4	P1.5	P1.6	P1.7	P1.8	P1.9	P1.10	P1.11	P1.12	P1.13
Эксперт1	0,087	0,087	0,099	0,065	0,076	0,065	0,076	0,076	0,076	0,065	0,087	0,076	0,065
Эксперт2	0,088	0,088	0,088	0,078	0,07	0,07	0,088	0,088	0,078	0,078	0,07	0,058	0,058
Эксперт3	0,073	0,084	0,084	0,073	0,095	0,084	0,073	0,084	0,06	0,06	0,073	0,073	0,084
Эксперт4	0,097	0,097	0,075	0,065	0,075	0,065	0,065	0,064	0,075	0,075	0,086	0,086	0,075
Значение коэффициента значимости	0,086	0,089	0,086	0,07	0,079	0,071	0,077	0,078	0,072	0,07	0,079	0,073	0,07

Для проведения оценки коэффициентов значимости основных показателей производного показателя P2 «Защита от вредоносного кода» экспертам представлено множество основных показателей P2.1 – P2.12. Результаты таковы.

Таблица 4 – Балльные оценки коэффициентов значимости основных показателей, выставленные экспертами

Э ОП	P2.1	P2.2	P2.3	P2.4	P2.5	P2.6	P2.7	P2.8	P2.9	P2.1 0	P2.1 1	P2.1 2
Эксперт1	9	8	8	7	8	9	7	8	6	8	6	8
Эксперт2	7	9	8	7	8	6	8	7	7	9	6	7
Эксперт3	9	8	7	8	6	8	6	8	9	8	9	8
Эксперт4	7	8	7	8	7	8	6	6	9	8	7	9

Таблица 5 – Оценки коэффициентов значимости для каждого основного показателя, вычисленные на основании балльных оценок коэффициентов значимости основных показателей, выставленных экспертами

Э ОП	P2.1	P2.2	P2.3	P2.4	P2.5	P2.6	P2.7	P2.8	P2.9	P2.1 0	P2.1 1	P2.1 2
Эксперт1	0,09 8	0,08 7	0,08 7	0,07 6	0,08 7	0,09 8	0,07 6	0,08 7	0,06 5	0,08 7	0,06 5	0,08 7
Эксперт2	0,07 9	0,1	0,09	0,07 9	0,09	0,06 7	0,09	0,07 9	0,07 9	0,1	0,06 7	0,07 9
Эксперт3	0,09 6	0,08 5	0,07 5	0,08 5	0,06 4	0,08 5	0,06 4	0,08 5	0,09 6	0,08 5	0,09 6	0,08 5
Эксперт4	0,07 8	0,08 9	0,07 8	0,08 9	0,07 8	0,08 9	0,06 7	0,06 7	0,1	0,08 9	0,07 8	0,1
Значение коэффициен та значимости	0,08 8	0,09	0,08 3	0,08 2	0,08	0,08 5	0,07 4	0,08	0,08 5	0,09	0,07 7	0,08 8

Для проведения оценки коэффициентов значимости основных показателей производного показателя РЗ «Защита информации при дистанционном режиме» экспертам представлено множество основных показателей РЗ.1 – РЗ.13. Результаты таковы.

Таблица 6 – Балльные оценки коэффициентов значимости основных показателей, выставленные экспертами

Э ОП	P3.1	P3.2	P3.3	P3.4	P3.5	P3.6	P3.7	P3.8	P3.9	P3.1 0	P3.1 1	P3.1 2	P3.1 3
Эксперт1	8	8	9	6	7	6	7	7	7	6	8	7	6
Эксперт2	9	9	9	8	7	7	9	9	8	8	7	6	6
Эксперт3	7	8	8	7	9	8	7	8	6	6	7	7	8
Эксперт4	9	9	7	6	7	6	6	6	7	7	8	8	7

Таблица 7 – Оценки коэффициентов значимости для каждого основного показателя, вычисленные на основании балльных оценок коэффициентов значимости основных показателей, выставленных экспертами

Э \ ОП	РЗ. 1	РЗ. 2	РЗ. 3	РЗ. 4	РЗ. 5	РЗ. 6	РЗ. 7	РЗ. 8	РЗ. 9	РЗ.1 0	РЗ.1 1	РЗ.1 2	РЗ.1 3
Эксперт1	0,08 7	0,08 7	0,09 9	0,06 5	0,07 6	0,06 5	0,07 6	0,07 6	0,07 6	0,06 5	0,08 7	0,07 6	0,06 5
Эксперт2	0,08 8	0,08 8	0,08 8	0,07 8	0,07	0,07	0,08 8	0,08 8	0,07 8	0,07 8	0,07	0,05 8	0,05 8
Эксперт3	0,07 3	0,08 4	0,08 4	0,07 3	0,09 5	0,08 4	0,07 3	0,08 4	0,06	0,06	0,07 3	0,07 3	0,08 4
Эксперт4	0,09 7	0,09 7	0,07 5	0,06 5	0,07 5	0,06 5	0,06 5	0,06 4	0,07 5	0,07 5	0,08 6	0,08 6	0,07 5
Значение коэффицие нта значимост и	0,08 6	0,08 9	0,08 6	0,07	0,07 9	0,07 1	0,07 7	0,07 8	0,07 2	0,07	0,07 9	0,07 3	0,07

Для проведения оценки коэффициентов значимости основных показателей производного показателя Р4 «Защита информационной инфраструктуры» экспертам представлено множество основных показателей Р4.1 – Р4.10. Результаты таковы.

Таблица 8 – Балльные оценки коэффициентов значимости основных показателей, выставленные экспертами

Э \ ОП	Р4.1	Р4.2	Р4.3	Р4.4	Р4.5	Р4.6	Р4.7	Р4.8	Р4.9	Р4.10
Эксперт1	7	7	9	6	7	8	8	8	7	9
Эксперт2	9	8	8	7	8	7	7	6	9	8
Эксперт3	9	6	8	8	8	9	8	8	9	8
Эксперт4	8	8	9	6	7	8	8	9	7	7

Таблица 9 – Оценки коэффициентов значимости для каждого основного показателя, вычисленные на основании балльных оценок коэффициентов значимости основных показателей, выставленных экспертами

Э ОП	P4.1	P4.2	P4.3	P4.4	P4.5	P4.6	P4.7	P4.8	P4.9	P4.10
Эксперт1	0,092	0,092	0,119	0,079	0,092	0,105	0,105	0,105	0,093	0,119
Эксперт2	0,117	0,104	0,104	0,091	0,104	0,091	0,091	0,078	0,117	0,104
Эксперт3	0,111	0,074	0,099	0,099	0,099	0,111	0,099	0,099	0,111	0,099
Эксперт4	0,104	0,104	0,117	0,078	0,091	0,104	0,104	0,117	0,091	0,091
Значение коэффициента значимости	0,106	0,094	0,11	0,087	0,097	0,103	0,1	0,1	0,103	0,103

1.5 Определение текущего уровня информационной безопасности объекта

Если оценка LT лежит в интервале от 0 до 0,25, то текущему уровню ИБ присваивается первый уровень.

Если оценка LT лежит в интервале от 0,25 до 0,5, то текущему уровню ИБ присваивается второй уровень.

Если оценка LT лежит в интервале от 0,5 до 0,7, то текущему уровню ИБ присваивается третий уровень.

Если оценка LT лежит в интервале от 0,7 до 0,85, то текущему уровню ИБ присваивается четвёртый уровень.

Если оценка LT лежит в интервале от 0,85 до 1, то текущему уровню ИБ присваивается пятый уровень.

2 Разработка способа оценки развития уровня ИБ

2.1 Разработка модели оценки развития уровня ИБ

Целью оценки развития уровня ИБ является определение возможности процессов управления информационной безопасностью (далее - процессов).

Для проведения оценки необходимо:

- определить структуру уровней возможности процессов и производных показателей возможности процессов для каждого уровня;
- разработать основные показатели возможности процессов;
- разработать способ измерения основных показателей возможности процессов;
- разработать шкалу измерения показателей возможности процессов;
- разработать способ формирования итоговой оценки возможности процессов.

На рисунке 2 представлена модель оценки возможности процессов управления ИБ.

Модель оценки возможности процессов управления информационной безопасностью показывает последовательность проведения оценки возможности любого процесса управления информационной безопасностью.

Для этого должны быть определены оцениваемые характеристики процесса. Оцениваемые характеристики процесса описываются основными показателями.

В качестве способа измерения основных показателей могут использоваться анкеты или метрики.

Функции формирования производных показателей процесса управления информационной безопасностью могут включать разнообразные способы, такие как усреднение результатов измерения, применение коэффициентов значимости основных показателей перед их объединением в производные показатели.



Рисунок 2 – Модель оценки возможности процессов управления ИБ

Модель формирования уровня возможности процесса позволяет определить достигнутый уровень возможности процесса по вычисленным производным показателям процесса.

Результаты оценки возможности процесса будут формироваться путем интерпретации их на основе критериев оценки возможности процесса. Для

этого должны быть идентифицированы и задокументированы основанные на целях информационной безопасности критерии оценки возможности процесса, которые устанавливают правила интерпретации результата оценки возможности процесса.

2.2 Требования к процессам управления информационной безопасностью

Для оценки возможности процессов управления ИБ выбраны следующие процессы:

- идентификация и определение ценности активов;
- идентификация и оценка угроз ИБ;
- идентификация и оценка уязвимостей активов;
- идентификация инцидентов ИБ;
- анализ рисков ИБ;
- оценивание рисков ИБ;
- обработка рисков ИБ.

Требования к указанным процессам (назначение, описание, результаты реализации процесса) представлены в Приложении В.

2.3 Разработка и описание способа оценки возможности процессов управления информационной безопасностью

2.3.1 Формирование структуры уровней возможности процессов и производных показателей возможности процессов для каждого уровня.

Уровень возможностей процесса управления ИБ – степень достижения процессом управления ИБ установленных целей в системе управления ИБ.

Для оценки возможностей процессов управления ИБ используются основные показатели процессов и производные показатели процессов. Производные показатели K_i (i – номер производного показателя) возможностей процессов управления ИБ отражают характеристики уровней возможностей процессов. Основные показатели процессов K_{ij} (i – номер производного показателя, j – номер основного показателя в производном показателе) входят в

состав производного показателя и детализируют характеристики уровней возможностей процессов, охватываемые производным показателем.

K_1 – Производный показатель Уровня 1

K_2 – Производный показатель Уровня 2

K_3 – Производный показатель Уровня 3

K_4 – Производный показатель Уровня 4

K_5 – Производный показатель Уровня 5

Уровень возможностей, достигнутый процессом, определяется оценками производных показателей процесса. Соответствие производных показателей процесса и их оценок уровням возможности процесса представлено в таблице 10.

Таблица 10 – Соответствие производных показателей процесса уровням возможности процесса

Уровень возможности процесса	Производный показатель процесса
Уровень 1	K_1
Уровень 2	K_1 K_2
Уровень 3	K_1 K_2 K_3
Уровень 4	K_1 K_2 K_3 K_4
Уровень 5	K_1 K_2 K_3 K_4 K_5

2.3.2 Разработка основных показателей возможности процессов.

На основе полного достижения характеристик процессов были сформированы основные показатели оценки возможности процессов управления информационной безопасностью. Основные показатели представлены в таблице 11.

Таблица 11 - Основные показатели оценки возможности процессов управления информационной безопасностью

Уровень возможностей процесса	Показатель процессов
K _{1.1}	Существуют ли меры и (или) средства, используемые для управления ИБ?
K _{1.2}	Достигают ли существующие меры и средства, используемые для управления ИБ, ожидаемого результата?
K _{1.3}	Реализована ли деятельность по управлению ИБ в виде процессов?
K _{2.1}	Организовано ли обучение принятым в организации процессам управления ИБ и информируются ли сотрудники об этих процессах?
K _{2.2}	Достигает ли процесс управления ИБ ожидаемых результатов?
K _{2.3}	Определен ли перечень нормативных документов организации, регулирующих процесс управления ИБ?
K _{3.1}	Зафиксирован ли документально процесс управления ИБ?
K _{3.2}	Существует ли в организации ролевая политика в области ИБ?
K _{3.3}	Определены ли цели осуществления процесса управления ИБ?
K _{3.4}	Определены ли ответственности и полномочия по осуществлению процесса управления ИБ?
K _{3.5}	Идентифицированы ли ресурсы и информация, необходимая для осуществления процесса управления ИБ?
K _{3.6}	Определен ли перечень результатов (выходов) процесса управления ИБ?
K _{3.7}	Формализована ли существующая в организации практика в области управления ИБ в виде процедур процесса управления ИБ?

Продолжение таблицы 11

К _{3.8}	Регламентирован ли в организации подход к обучению и информированию о реализованном процессе управления ИБ?
К _{3.9}	Установлены ли в организации требования по осуществлению контроля за реализацией процесса управления ИБ?
К _{3.10}	Осуществляется ли в организации оценка процесса управления ИБ?
К _{4.1}	Установлена ли (документально зафиксирована) в организации ответственность за процесс управления ИБ (распределены роли по обеспечению ИБ, назначены исполнители ролей и т.п.)?
К _{4.2}	Доведены ли ответственность и полномочия по осуществлению процесса ИБ до сведения ответственных лиц в организации?
К _{4.3}	Компетентен ли персонал, осуществляющий процесс управления ИБ?
К _{4.4}	Регламентирован ли в организации процесс управления ИБ?
К _{4.5}	Существует ли в организации контроль за исполнением требований всех нормативных документов организации и нормативных документов внешних регулирующих и надзорных органов в области ИБ?
К _{4.6}	Соответствует ли процесс управления ИБ общепринятой практике?
К _{4.7}	Доступны ли ресурсы и информация, необходимая для осуществления процесса управления ИБ?
К _{4.8}	Определены ли соответствующие методы для проведения измерения (оценки) процесса управления ИБ?
К _{4.9}	Реализован ли постоянный контроль за реализацией процесса управления ИБ?
К _{4.10}	Существует ли возможность принятия мер в случае, если процесс управления ИБ неэффективен?
К _{4.11}	Осуществляется ли совершенствование процесса управления ИБ регламентированным образом?
К _{5.1}	Определены ли цели улучшения процессов и процедур управления ИБ, которые обеспечивают достижение целей деятельности организации?

K _{5.2}	Идентифицированы ли возможности улучшений, связанные с новыми технологиями?
K _{5.3}	Направлено ли непрерывное совершенствование ИБ на совершенствование процессов и процедур управления ИБ?

При формировании оценки для различных процессов управления ИБ основные показатели обозначаются с дополнительным индексом, определяющим оцениваемый процесс управления ИБ, - K_{ij}^p , где i – индекс производного показателя, j – индекс основного показателя, p – индекс оцениваемого процесса управления ИБ.

2.3.3 Разработка способа измерения основных показателей возможности процессов.

Измерения и последующая оценка процессов проводится в соответствии с моделью оценки процесса, основой которой является совокупность анкет для оценки процессов управления ИБ.

Анкеты для оценки основных показателей процессов приведены в Приложении Г.

Оценка основных показателей процессов управления ИБ производится с помощью упорядоченной шкалы, отражающей уровень реализации характеристик оцениваемого процесса.

Используются следующие обозначения значений оценки:

Н – не выполнен. Свидетельств выполнения основного показателя мало или они отсутствуют.

Ч – частично выполнен. Имеются свидетельства частичного, некоторого выполнения основного показателя.

В – в основном выполнен. Имеются свидетельства систематического подхода к выполнению и существенного выполнения основного показателя. В оцениваемой характеристике процесса возможны некоторые слабые места.

П – полностью выполнен. Имеются свидетельства полного и систематического подхода и полного выполнения основного показателя. В оцениваемой характеристике процесса нет существенных слабых мест.

Уровень выполнения основного показателя в представленной шкале следует выражать в процентах выполнения:

Н – не выполнен [0% - 15%];

Ч – частично выполнен (15% - 50%];

В – в основном выполнен (50% - 85%];

П – полностью выполнен (85% - 100%].

Объединение оценок основных показателей в оценку производного показателя осуществляется по следующему правилу:

— производный показатель имеет оценку П (полностью выполнен), если 50% и выше основных показателей имеют оценку П (полностью выполнен), а остальные показатели – оценку В (в основном выполнен);

— производный показатель имеет оценку В (в основном выполнен), если 50% и выше показателей имеют оценку В (в основном выполнен), а остальные показатели – оценку Ч (частично выполнен);

— производный показатель имеет оценку Ч (частично выполнен), если 50% и выше показателей имеют оценку Ч (частично выполнен);

— в остальных случаях производный показатель имеет оценку Н (не выполнен).

Достигнутый процессом управления ИБ уровень возможности формируется из оценок производных показателей в соответствии с моделью формирования уровня возможности процесса.

2.3.4 Разработка способа формирования оценки возможности процессов.

Для формирования итоговой оценки возможности процессов должны быть определены:

1. Модель формирования уровня возможности процесса;
2. Критерии оценки возможности процесса.

Модель формирования уровня возможности процесса представляется соответствием производных показателей процесса и их оценок уровням возможности процесса (Таблица 12).

Таблица 12 - Модель формирования уровня возможности процесса

Уровень возможностей процесса	Производный показатель процесса	Оценка производного показателя
Уровень 1	K_1	В основном выполнен или полностью выполнен
Уровень 2	K_1	Полностью выполнен
	K_2	В основном выполнен или полностью выполнен
Уровень 3	K_1	Полностью выполнен
	K_2	Полностью выполнен
	K_3	В основном выполнен или полностью выполнен
Уровень 4	K_1	Полностью выполнен
	K_2	Полностью выполнен
	K_3	Полностью выполнен
	K_4	В основном выполнен или полностью выполнен
Уровень 5	K_1	Полностью выполнен
	K_2	Полностью выполнен
	K_3	Полностью выполнен
	K_4	Полностью выполнен
	K_5	В основном выполнен или полностью выполнен

Критерии оценки возможности процесса определяют, являются ли оцениваемые процессы управления информационной безопасностью приемлемыми или неприемлемыми. Например, критерии оценки возможности процессов могут быть такими. Уровни возможности процессов управления

информационной безопасностью Y4 и Y5 являются приемлемыми, уровни возможности процессов Y1, Y2, Y3 являются неприемлемыми.

2.3.5 Формирование итоговой оценки возможности процессов.

В результате оценки возможности процессов управления ИБ определяется уровень Y возможности каждого процесса.

Итоговая оценка LB уровня возможности процессов устанавливается наименьшей из всех полученных оценок:

$$LB = \min_i Y_i$$

3 Формирование итоговой оценки уровня ИБ объекта

Итоговая оценка L уровня ИБ объекта формируется в соответствии с моделью, представленной на рис. 3 .

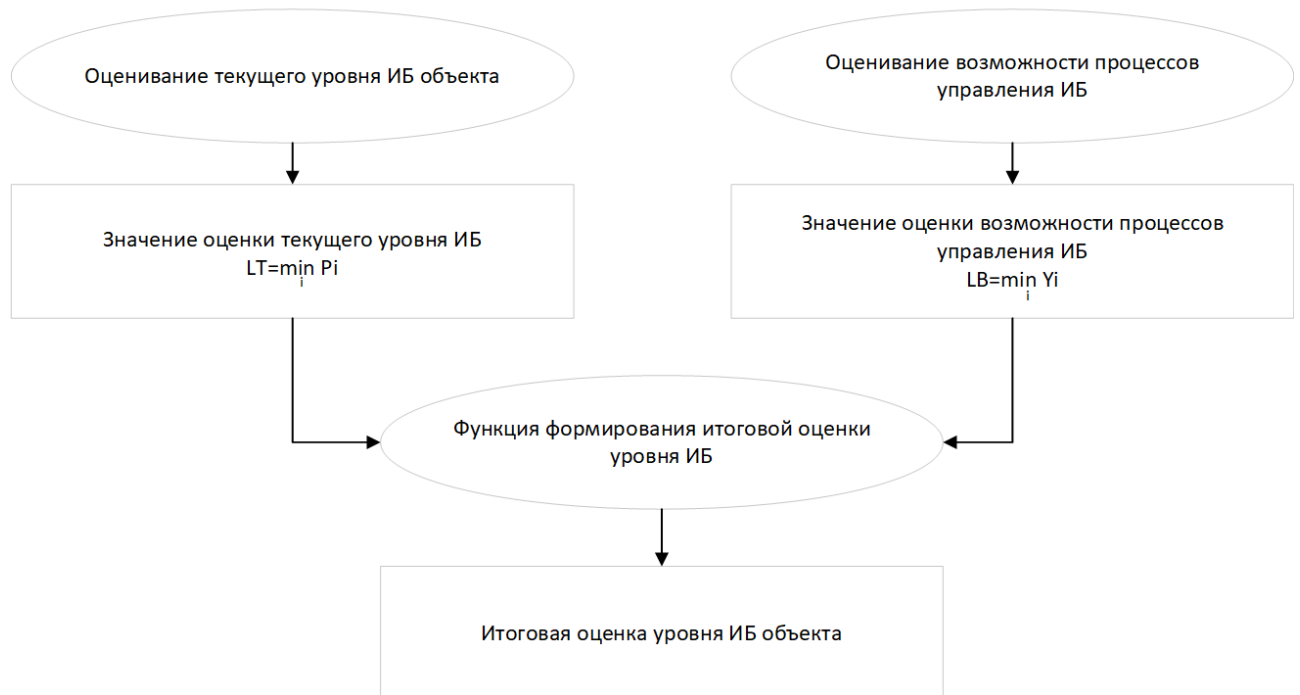


Рисунок 3 – Модель итоговой оценки уровня ИБ объекта

Функцией формирования итоговой оценки уровня ИБ объекта является функция определения наименьшей оценки из оценок уровней LT и LB :

$$L = \min LT, LB$$

4 Разработка и описание методики оценки ИБ объекта

Методика оценки уровня ИБ объекта формируется на основе разработанных способов оценки текущего уровня ИБ и оценки возможности процессов управления ИБ.

Методика оценки уровня ИБ объекта включает следующие разделы:

1. Общие положения:

- а) цель и задачи оценки уровня ИБ объекта;
- б) формы проведения оценки (внутренняя, внешняя).

2. Способ оценки текущего уровня ИБ:

- а) оценивание основных и производных показателей текущего уровня ИБ;
- б) формирование итоговой оценки текущего уровня ИБ.

3. Способ оценки возможности процессов управления ИБ:

- а) структура уровней возможности процессов;
- б) оценивание основных и производных показателей процессов управления ИБ;
- в) формирование итоговой оценки возможности процессов управления ИБ.

4. Формирование итоговой оценки уровня ИБ объекта.

5 Вредные психофизиологические факторы, влияющие на психоэмоциональное состояние специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

5.1 Вредные психофизиологические факторы, влияющие на психоэмоциональное состояние специалиста по защите информации

Согласно ГОСТ 12.0.003-2015 среди производственных факторов, оказывающих отрицательное психофизиологическое воздействие на организм человека, выделяют:

- физические перегрузки, определяемые тяжестью трудового процесса;
- нервно-психические перегрузки, определяемые напряженностью трудового процесса.

К физическим перегрузкам относятся:

- статические нагрузки, определяемые рабочей позой;
- динамические нагрузки, определяемые массой поднимаемого и перемещаемого вручную груза;
- динамические нагрузки, определяемые повторением монотонных рабочих движений.

В своей работе специалист по защите информации связан только с одним видом вредных психофизиологических факторов - статическими перегрузками, определяемые рабочей позой, так как проводит большую часть рабочего времени за компьютером в одном положении.

Среди нервно-психических перегрузок выделяют:

- умственное перенапряжение, в том числе связанное с информационной нагрузкой;
- чрезмерное напряжение анализаторов, также вызванное информационной перегрузкой;
- монотонность труда, способствующая формированию монотонии, то есть снижению работоспособности в результате выполнения однообразной работы, связанной с частым повторением стереотипных действий;

– эмоциональные перегрузки.

Специалист по защите информации подвержен всем видам нервно-психических перегрузок, так как его деятельность включает работу с большим количеством информации и высокую степень ответственности. Ухудшению психоэмоционального состояния в этом случае способствует повышенное зрительное перенапряжение, умственные и нервно-эмоциональные нагрузки, продолжительная концентрация внимания, монотонность трудового процесса, большой объем информации, нерациональная организация рабочего места.

Таким образом, нервно-психические перегрузки в работе специалиста по защите информации - это следствие информационного взаимодействия в системе «пользователь – ПЭВМ». Они определяются некачественными условиями передачи изображения, несоответствием некоторых параметров информационных систем психофизиологическими особенностями человека, необходимостью внимательного наблюдения за информационными знаками, быстрого анализа постоянно изменяющейся информации, принятия продуктивных решений и выполнения определённых корректирующих действий.

Как правило, операторы ПЭВМ жалуются к концу рабочего дня на зрительное переутомление, головную боль, ноющие боли в мышцах шеи, плечевого пояса и спины, снижение способности к концентрации внимания.

Ухудшение самочувствия пользователя ПЭВМ при длительной работе связано также повышением пульсации потоков света от источников искусственного освещения и монитора. Пульсации потоков света способствуют повышению общего и зрительного переутомления, ухудшению зрительной и общей работоспособности. При уменьшении частоты световых пульсаций вредное воздействие усиливается. К нервно-психическим факторам относится также низкочастотное мерцание экрана (до 200 Гц), то есть кажущееся изменение яркости свечения.

Оно возникает из-за взаимодействия пульсирующих потоков света экрана и источников света. Даже на начальном этапе компьютеризации общества было обнаружено специфическое зрительное утомление при работе за дисплеем, которое было названо «компьютерный зрительный синдром. Это объясняется тем, что у человека зрительная система по ходу эволюции приспособилась для восприятия изображения в отраженном свете (напечатанная информация, тексты, рисунки), а не для работы за монитором компьютера. Изображение на дисплее сильно отличается от привычного глазу объектов внешнего мира — оно светится, мерцает, состоит из дискретных точек, кроме этого цвета компьютерного изображения отличаются от естественных цветов. Однако зрительное переутомление вызывают не только особенности изображения на экране. Сильная нагрузка на глаза оказывается при введении информации, так как пользователю необходимо переводить часто взгляд с экрана на набираемый текст и клавиатуру, которые находятся на разном расстоянии от монитора и по-разному освещены. Зрительное переутомление обычно проявляется при затуманивании зрения, сопровождается трудностями при переносе взгляда с близких предметов на дальние и с дальних на близкие, кажущееся изменение цвета предметов, двоение предметов, чувством жжения, «песка» в глазах, болезненными ощущениями при движении глаз, покраснением век.

Специфическое воздействие электромагнитного поля выражается в биохимических изменениях, происходящие в клетках и тканях. Наиболее подвержены данным воздействиям центральная и сердечнососудистая системы. Могут наблюдаться отклонения в работе эндокринной системы. В начале воздействия отмечается повышение возбудимости нервной системы, проявляющееся повышением раздражительности, нарушением сна, эмоциональной неуравновешенностью. Затем развиваются астенические проявления, т.е. физическая и нервно-психическая слабость. В целом хроническое воздействие ЭМП проявляется следующими симптомами: головная боль, повышенная утомляемость, ухудшение самочувствия,

брадикардия (урежение пульса), а также гипотония (понижение артериального давления), боли в сердце. Данные негативные симптомы могут выражаться в разной степени.

5.2 Методы и средства физической культуры, снижающие воздействие вредных психофизиологических факторов

Для нормального функционирования мозга необходимо, чтобы к нему поступали нервные импульсы от всех систем организма, в том числе и от мышц, которые составляют половину от массы всего организма. Движения мышц создают огромный поток нервных импульсов, способствующих обогащению мозга разнообразными ощущениями, поддерживающих его в хорошем рабочем состоянии. Именно поэтому умственная работоспособность непосредственно связана с общим состоянием здоровья, в укреплении которого важная роль отводится физической культуре.

При умственном труде, который лежит в основе деятельности специалиста по защите информации, в коре головного мозга формируются замкнутые циклы возбуждения, которые характеризуются большой устойчивостью и инертностью. Поэтому, если после прекращения физической нагрузки человек практически сразу может переключиться на новый вид деятельности, то при умственном труде интенсивная работа мозга не заканчивается продолжительное время и после завершения интеллектуальной нагрузки.

В основе организации отдыха при умственных перегрузках лежит принцип активного отдыха, который предусматривает систему организованных движений до, в процессе и по окончании умственного деятельности, что оказывает благоприятный эффект не только в сохранении, но и повышении умственной работоспособности. Ежедневные и регулярные физические упражнения способствуют формированию в коре больших полушарий «доминанты движения», которая оказывает положительное воздействие на состояние дыхательной, мышечной, сердечнососудистой систем организма, активизирует зону сенсомоторной активности в коре головного мозга, способствует повышению тонуса всего организма.

Перед началом интенсивной умственной работы, для сокращения периода вработывания, рекомендуются в течение 5 минут произвольные движения

умеренной или средней интенсивности, направленные на дополнительное напряжение мышц конечностей. При этом чем ниже исходное нервно-психическое и мышечное напряжение человека, и чем быстрее необходимо включиться в работу, тем интенсивнее должно быть упражнения на напряжение скелетных мышц. В процессе напряженной продолжительной умственной деятельности, сопровождаемой к тому же эмоциональным стрессом, рекомендуется проделать произвольные упражнения на общее расслабление и снижение тонуса скелетных мышц, желательно в сочетании с ритмичным сокращением небольших мышечных групп (разгибателей и сгибателей пальцев кисти, мимических мышц лица и т. п.).

Для повышения работоспособности мозга на фоне мышечного расслабления, улучшения функций дыхания и кровообращения, необходимо регулярно выполнять кратковременные физические упражнения. Например, раз в час при работе за компьютером проделать познотонические упражнения в течении нескольких минут. а через каждые 2 ч желательно проводить минутные динамические упражнения, такие как бег на месте, с ритмичным, глубоким дыханием.

Для снижения напряжения глаз каждые 2 часа рекомендуется выполнять упражнения для глаз. Гимнастику для глаз за компьютером лучше выполнять в расслабленном состоянии. При наличии боли в области шеи или спины, необходимо сначала выполнить упражнения для этих зон. При выполнении упражнений для глаз надо глубоко дышать, так как при работе глазные мышцы должны активно насыщаться кислородом.

Правильно подобранный комплекс упражнений повышает общий эмоциональный тонус работника, создавая устойчивое настроение, которое станет благоприятным фоном для активной умственной деятельности и необходимо для предупреждения раннего развития утомления. Физическая нагрузка выстроенная на основе принципа активного отдыха, оказывает благоприятное воздействие на повышение умственной работоспособности специалиста по защите информации.

Заключение

В результате выполнения дипломной работы была разработана методика оценки ИБ объекта.

В первом разделе ВКР была произведена разработка способа оценки текущего уровня ИБ.

Во втором разделе ВКР была произведена разработка способа оценки развития уровня ИБ.

В третьем разделе описано формирование итоговой оценки уровня ИБ объекта.

В четвертом разделе была разработана и описана методика оценки ИБ объекта.

В приложении А представлены требования ИБ для областей обеспечения ИБ.

В приложении Б представлены анкеты для оценки показателей ИБ.

В приложении В представлены требования к процессам управления ИБ.

В приложении Г представлены анкеты для оценки основных показателей процессов управления ИБ.

Таким образом, все пункты технического задания на выпускную квалификационную работу выполнены полностью.

Список использованных источников

- 1 Международный стандарт ИСО/МЭК 15504 – 1:2004 «Информационная технология. Оценка процесса. Понятия и терминология».
- 2 ГОСТ Р ИСО/МЭК 27001 - 2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности»;
- 3 ГОСТ Р ИСО/МЭК 27002 -2012 «Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»;
- 4 Международный стандарт ИСО/МЭК 15504 – 3:2004 «Информационная технология. Оценка процесса. Руководство по проведению оценки»;

Приложение А

(обязательное)

Требования ИБ для областей обеспечения ИБ

А.1 Требования по обеспечению защиты информации при управлении доступом

1. Должен быть документально определен перечень информационных активов (их типов) организации. Права доступа работников организации к данным активам должны быть документально зафиксированы.

2. В организации должны быть документально определены, выполняться и контролироваться процедуры идентификации, аутентификации, авторизации; управления доступом; контроля целостности; регистрации событий и действий.

Результаты контроля процедур должны документироваться.

3. В организации необходимо документально определить и использовать процедуры мониторинга и анализа данных регистрации, действий и операций, позволяющие выявлять неправомерные или подозрительные операции.

Процедуры мониторинга и анализа должны использовать документально определенные критерии выявления неправомерных или подозрительных действий и операций. Процедуры мониторинга и анализа должны применяться на регулярной основе, например, ежедневно, ко всем выполненным операциям.

4. Порядок доступа работников организации в помещения, в которых размещаются объекты среды информационных активов, должен быть регламентирован во внутренних документах организации, а его выполнение должно контролироваться.

Результаты контроля выполнения порядка доступа должны оформляться документально.

5. Должны быть документально оформлены и доведены до сведения работников организации процедуры, определяющие действия в случае компрометации информации, необходимой для их идентификации,

аутентификации и(или) авторизации, в том числе произошедшей по их вине, включая информацию о способах распознавания таких случаев.

Эти процедуры должны предусматривать документирование работниками всех своих действий и их результатов.

6. В организации должны применяться защитные меры, направленные на обеспечение защиты от НСД и НРД, повреждения или нарушения целостности информации, необходимой для регистрации, идентификации, аутентификации и(или) авторизации клиентов и работников организации. Все попытки НСД и НРД к такой информации должны регистрироваться. При увольнении или изменении должностных обязанностей работников организации, имевших доступ к указанной информации, необходимо выполнить документированные процедуры соответствующего пересмотра прав доступа.

7. Работа всех пользователей АС должна осуществляться под уникальными учетными записями.

А.2 Требования по обеспечению защиты информации при защите от вредоносного кода

1. На всех автоматизированных рабочих местах и серверах АС организации должны применяться средства защиты от вредоносного кода.

Процедуры установки и регулярного обновления средств защиты от вредоносного кода (версий и баз данных) на автоматизированных рабочих местах и серверах АС должны быть документированы и осуществляться администраторами АС или иными официально уполномоченными лицами.

Установка и обновление средств защиты от вредоносного кода в организации должны контролироваться представителями подразделения (лицами) в организации, ответственными за обеспечение ИБ.

2. Должны быть разработаны и введены в действие инструкции по защите от вредоносного кода.

3. В организации должна быть организована защита от вредоносного кода всего трафика электронного почтового обмена.

4. Рекомендуется организовать построение централизованной системы антивирусной защиты, предусматривающей использование средств защиты от вредоносного кода различных производителей и их отдельную установку на рабочих станциях, почтовых серверах и межсетевых экранах.

5. Должны быть документально определены и выполняться процедуры предварительной проверки устанавливаемого или изменяемого программного обеспечения на отсутствие вредоносного кода. После установки или изменения программного обеспечения должна быть выполнена проверка наличия вредоносного кода. Результаты установки, изменения программного обеспечения и проверки наличия вредоносного кода должны документироваться.

6. Должны быть документально определены процедуры, выполняемые в случае обнаружения вредоносного кода, в которых, в частности, должны быть зафиксированы:

— необходимые меры по отражению и устранению последствий внедрения вредоносного кода;

— порядок официального информирования руководства;

— порядок приостановления при необходимости работы (на период устранения последствий внедрения вредоносного кода).

7. Должны быть документально определены и выполняться процедуры контроля за отключением и обновлением средств защиты от вредоносного кода на всех автоматизированных рабочих местах и серверах АС. Результаты контроля должны документироваться.

8. Ответственность за выполнение требований по защите от вредоносного кода должна быть возложена на руководителя функционального подразделения организации, а обязанности по выполнению предписанных мер защиты от вредоносного кода должны быть возложены на каждого работника организации, имеющего доступ к ЭВМ и (или) АС.

А.3 Требования по обеспечению защиты информации при дистанционном режиме

1. Должны быть документально определены перечень работ, которые разрешены для проведения в дистанционном режиме.

2. В организации должно быть документально определено и установлено время работы.

3. Необходимо определить и зафиксировать документально классификацию информации, которая может поддерживаться внутренними системами и услугами, к которым разрешен доступ сотруднику в дистанционном режиме.

4. Должен быть документально оформлен перечень нарушений, за которые производится аннулирование полномочий.

5. Должен быть документально оформлен перечень нарушений, за которые производится отмена прав доступа.

6. В организации должен быть документально оформлен перечень действий по возвращению оборудования в случае прекращения работы в дистанционном режиме.

7. Должен быть определен перечень коммуникационных технологий, применяющихся при работе в дистанционном режиме, дающие возможность сотрудникам работать в конкретном удаленном месте за пределами своей организации.

А.4 Требования по обеспечению защиты информации информационной инфраструктуры

1. В организации должен быть документально определен список лиц, которым разрешены действия по внесению изменений в конфигурацию информационной инфраструктуры.

2. Должно проводиться резервирование информационной инфраструктуры, необходимой для функционирования технических мер защиты информации.

3. Должны быть документально определен перечень регламентированных мер по восстановлению отказавших технических мер защиты информации информационной инфраструктуры, необходимых для их функционирования.

4. Необходимо осуществлять контроль фактического размещения технических мер защиты информации в информационной инфраструктуре.

5. Необходимо осуществлять организацию и контроль размещения, хранения и обновления ПО информационной инфраструктуры.

6. Должен осуществляться контроль состава и целостности ПО информационной инфраструктуры.

7. Необходимо документально фиксировать регистрацию событий защиты информации, связанных с результатами контроля целостности и защищенности информационной инфраструктуры.

8. Необходимо осуществлять контроль фактических параметров настроек технических мер защиты информации и компонентов информационной инфраструктуры, предназначенных для размещения технических мер защиты информации.

9. Необходимо осуществлять регистрацию операций по изменению параметров настроек технических мер защиты информации и информационной инфраструктуры, предназначенных для размещения технических мер защиты информации.

Приложение Б

(обязательное)

Показатели информационной безопасности

Таблица Б.1 – Производный показатель Р1 «Защита информации при управлении доступом»

Обозначение основного показателя	Основной показатель	Оценка основного показателя					Коэффициент значимости основного показателя	Вычисленное значение основного показателя
		0	0.25	0.5	0.75	1		
Р1.1	Определены ли документально перечень информационных активов (их типов) объекта и зафиксированы ли документально права доступа работников объекта к данным активам?						0,086	
Р1.2	Определены ли документально перечень защитных мер от НСД?						0,089	
Р1.3	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры идентификации, аутентификации, авторизации субъектов доступа, в том числе внешних субъектов доступа, которые не являются работниками организации?						0,086	

Обозначение основного показателя	Основной показатель	Оценка показателя основного					Коэффициент значимости основного показателя	Вычисленное значение основного показателя
		0	0.25	0.5	0.75	1		
P1.4	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры выявления и блокирования неуспешных попыток доступа?						0,07	
P1.5	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры выявления и блокирования несанкционированного перемещения (копирования) информации, в том числе баз данных, файловых ресурсов, виртуальных машин?						0,079	
P1.6	Используются ли для проведения процедур мониторинга ИБ и анализа данных о действиях и операциях специализированные программные и (или) технические средства?						0,071	

Обозначение основного показателя	Основной показатель	Оценка показателя основного					Коэффициент значимости основного показателя	Вычисленное значение основного показателя
		0	0.25	0.5	0.75	1		
P1.7	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры блокирования сеанса доступа после установленного времени бездействия или по запросу субъекта доступа, требующего выполнения процедур повторной аутентификации и авторизации для продолжения работы?						0,077	
P1.8	Определены ли действия и операции, подлежащие регистрации?						0,078	
P1.9	Определены ли сроки хранения действий и операций, подлежащих регистрации?						0,072	
P1.10	Обеспечено ли резервирование необходимого объема памяти для записи данных?						0,07	

Обозначение основного показателя	Основной показатель	Оценка показателя основного					Коэффициент значимости основного показателя	Вычисленное значение основного показателя
		0	0.25	0.5	0.75	1		
P1.11	Определены ли, выполняется ли, регистрируется ли и контролируется ли порядок доступа к объектам среды информационных активов, в том числе в помещения, в которых размещаются объекты среды информационных активов?						0,079	
P1.12	Определены ли, выполняется ли и контролируется ли в организации порядок использования съемных носителей информации?						0,073	
P1.13	Предоставляется ли доступ к данным о действиях и операциях только с целью выполнения служебных обязанностей?						0,07	

Таблица Б.2 – Производный показатель Р2 «Защита информации от вредоносного кода»

Обозначение основного показателя	Основной показатель	Оценка основного показателя					Коэффициент значимости основного показателя	Вычисленное значение основного показателя
		0	0.25	0.5	0.75	1		
P2.1	Применяются ли на всех автоматизированных рабочих местах организации, если иное не предусмотрено технологическим процессом, средства антивирусной защиты?						0,088	
P2.2	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации процедуры установки и регулярного обновления средств антивирусной защиты (версий и баз данных) на автоматизированных рабочих местах?						0,09	
P2.3	Организовано ли функционирование постоянной антивирусной защиты в автоматическом режиме и автоматический режим установки обновлений антивирусного программного обеспечения и его баз данных?						0,083	

Обозначение основного показателя	Основной показатель	Оценка показателя основного					Коэффициент значимости основного показателя	Вычисленное значение основного показателя
		0	0.25	0.5	0.75	1		
P2.4	Проводится ли антивирусная проверка съемных носителей информации перед их подключением к средствам вычислительной техники, задействованным в рамках осуществления технологических процессов, на специально выделенном автономном средстве вычислительной техники?						0,082	
P2.5	Разработаны ли и введены ли в действие инструкции и рекомендации по антивирусной защите, учитывающие особенности технологических процессов?						0,08	
P2.6	Организована ли в организации антивирусная фильтрация всего трафика электронного почтового обмена?						0,085	

Обозначение основного показателя	Основной показатель	Оценка показателя основного					Коэффициент значимости основного показателя	Вычисленное значение основного показателя
		0	0.25	0.5	0.75	1		
P2.7	Организована ли в организации эшелонированная централизованная система антивирусной защиты, предусматривающая использование средств антивирусной защиты различных производителей на: - рабочих станциях; - серверном оборудовании, в том числе серверах электронной почты; - технических средствах межсетевого экранирования?						0,074	
P2.8	Определены ли, выполняются ли, регистрируются ли и контролируются ли процедуры предварительной проверки устанавливаемого или изменяемого программного обеспечения на отсутствие вирусов?						0,08	
P2.9	Выполняется ли после установки или изменения программного обеспечения антивирусная проверка?						0,085	

Обозначение основного показателя	Основной показатель	Оценка показателя основного					Коэффициент значимости основного показателя	Вычисленное значение основного показателя
		0	0.25	0.5	0.75	1		
P2.10	Определены ли, выполняются ли, регистрируются ли и контролируются ли процедуры, выполняемые в случае обнаружения компьютерных вирусов, в которых, в частности, необходимо зафиксировать: - необходимые меры по отражению и устранению последствий вирусной атаки; - порядок официального информирования руководства; - порядок приостановления при необходимости работы (на период устранения последствий вирусной атаки)?						0,09	
P2.11	Определены ли, выполняются ли и регистрируются ли процедуры контроля за отключением и обновлением антивирусных средств на всех технических средствах?						0,077	

Обозначение основного показателя	Основной показатель	Оценка показателя основного					Коэффициент значимости основного показателя	Вычисленное значение основного показателя
		0	0.25	0.5	0.75	1		
P2.12	Возложена ли обязанность по выполнению предписанных мер антивирусной защиты на каждого работника организации, имеющего доступ к ЭВМ, а ответственность за выполнение требований по антивирусной защите - на руководителей функциональных подразделений организации?						0,088	

Таблица Б.3 – Производный показатель РЗ «Защита информации при дистанционном режиме»

Обозначение основного показателя	Основной показатель	Оценка основного показателя					Коэффициент значимости и основного показателя	Вычисленное значение основного показателя
		0	0.25	0.5	0.75	1		
РЗ.1	Определены ли документально перечень работ, которые могут проводиться в дистанционном режиме?						0,086	
РЗ.2	Проведен ли инструктаж работников осуществляющих взаимодействие с ЭВМ в дистанционном режиме?						0,089	
РЗ.3	Определены ли перечень технических средств, в том числе портативных вычислительных средств, которые будут предоставлены работникам во время дистанционного режима?						0,086	
РЗ.4	Определены ли перечень информации и информационных ресурсов к которым должен предоставляться доступ?						0,07	
РЗ.5	Определены ли права привилегии для работников во время дистанционного режима?						0,079	

Обозначение основного показателя	Основной показатель	Оценка показателя основного					Коэффициент значимости и основного показателя	Вычисленное значение основного показателя
		0	0.25	0.5	0.75	1		
P3.6	Определены ли документально перечень мероприятий по исключению возможности эксплуатации задействованных средств вычислительной техники на время дистанционного режима?						0,071	
P3.7	Составлен ли “Белый список” физических (MAC) адресов для идентификации средств вычислительной техники при взаимодействии с информационными ресурсами на время дистанционного режима?						0,077	
P3.8	Реализована ли двухфакторная аутентификация работников при использовании средств вычислительной техники на время дистанционного режима?						0,078	
P3.9	Определены ли документально перечень информации и информационных ресурсов доступ к которым осуществляется через VPN-клиент?						0,072	
P3.10	Обеспечено ли резервирование необходимого объема памяти для записи данных?						0,07	

Обозначение основного показателя	Основной показатель	Оценка показателя основного					Коэффициент значимости и основного показателя	Вычисленное значение основного показателя
		0	0.25	0.5	0.75	1		
P3.11	Определены ли документально перечень средств антивирусной защиты, необходимых для использования на средствах вычислительной техники во время дистанционного режима?						0,079	
P3.12	Реализована ли защита от установки работниками программного обеспечения на удаленные средства вычислительной техники?						0,073	
P3.13	Определено ли время неактивности работника, по истечении которого будет выполнено блокирование сеанса?						0,07	

Таблица Б.4 – Производный показатель Р4 «Защита информационной инфраструктуры»

Обозначение основного показателя	Основной показатель	Оценка основного показателя					Коэффициент значимости и основного показателя	Вычисленное значение основного показателя
		0	0.25	0.5	0.75	1		
Р4.1	Определены ли документально список лиц, которым разрешены действия по внесению изменений в конфигурацию информационной инфраструктуры?						0,106	
Р4.2	Определены ли документально перечень мероприятий по резервированию информационной инфраструктуры?						0,094	
Р4.3	Определены ли документально перечень мер по восстановлению отказавших технических мер по защите информации информационной инфраструктуры?						0,11	
Р4.4	Определены ли список работников ответственных за восстановление отказавших технических мер по защите информации информационной инфраструктуры?						0,087	
Р4.5	Определены ли документально перечень мер по контролю фактического размещения технических мер по защите информации информационной инфраструктуры?						0,097	

Обозначение основного показателя	Основной показатель	Оценка показателя основного					Коэффициент значимости и основного показателя	Вычисленное значение основного показателя
		0	0.25	0.5	0.75	1		
P4.6	Определены ли документально перечень мероприятий по организации и контролю размещения, хранения и обновления ПО информационной инфраструктуры?						0,103	
P4.7	Определены ли документально перечень мероприятий по контролю состава и целостности ПО информационной инфраструктуры?						0,1	
P4.8	Определены ли документально перечень мероприятий по фиксированию регистрации событий защиты информации, связанных с результатами контроля целостности и защищенности информационной инфраструктуры?						0,1	
P4.9	Определены ли документально перечень фактических параметров настроек технических мер защиты информации и компонентов информационной инфраструктуры, предназначенных для размещения технических мер защиты информации?						0,103	

Обозначение основного показателя	Основной показатель	Оценка показателя основного					Коэффициент значимости и основного показателя	Вычисленное значение основного показателя
		0	0.25	0.5	0.75	1		
P4.10	Осуществляется ли регистрация операций по изменению параметров настроек технических мер защиты информации и информационной инфраструктуры, предназначенных для размещения технических мер защиты информации?						0,103	

Приложение В

(обязательное)

Требования к процессам управления информационной безопасностью

В.1 Идентификация и определение ценности активов

Основной целью идентификации активов является определение наиболее важных с точки зрения целей деятельности организации активов. Оценка важности идентифицированных активов проводится в рамках процесса оценки рисков.

Для каждого актива определяется его тип, бизнес-процесс, в котором он участвует, используемое техническое средство, подразделение, в котором данный актив обрабатывается. С помощью определения влияния различных факторов на актив вычисляются соответствующие значения оценки важности.

Результатом данного процесса является сформированный перечень активов, оцененных с точки зрения их важности для организации и классификации по их возможным типам.

В.2 Идентификация и оценка угроз ИБ

Угроза обладает потенциалом причинения вреда активам, таким, как информация, процессы и системы, а, следовательно, и самой организации. При идентификации должны быть учтены все возможные источники угроз активам.

Используемыми данными для идентификации угроз информационной безопасности, актуальных для идентифицированных активов, являются:

- перечень активов, оцененных с точки зрения их важности для организации и классифицированных по их возможным типам;
- перечень типовых угроз информационной безопасности объекта защиты;
- перечень угроз, зафиксированный в результате обработки инцидентов ИБ;

— относительная частота реализации угроз, зафиксированных в результате обработки инцидентов;

— перечень уязвимостей, имеющих место у активов объекта оценки и являющихся для них потенциально опасными;

— информация об источнике угрозы.

Эксперты совместно с владельцами и/или пользователями активов для идентификации угроз ИБ активов объекта оценки выполняют следующие действия:

— для каждого идентифицированного актива, входящего в состав объекта оценки указываются угрозы, которые могут нарушить свойства ИБ активов объекта оценки, то есть являются потенциально опасными для объекта оценки;

— для каждой угрозы определяется один или несколько потенциальных источников, причем, для источника антропогенного характера применяются формальная модель нарушителя;

— указывается метод реализации угрозы, доступный источнику угрозы и сложность обнаружения реализации угрозы;

— выбирается одна или несколько уязвимостей рассматриваемого актива, пригодных для реализации угрозы.

При рассмотрении угрозы ИБ, выявленной на основании результатов обработки инцидентов ИБ для неё рассчитывается относительная частота реализации. Для этого определяется общее количество инцидентов ИБ, в которых были выявлены все зафиксированные угрозы ИБ. Затем определяется количество инцидентов ИБ, в которых была зафиксирована рассматриваемая угроза. Относительная частота реализации рассматриваемой угрозы определяется соотношением количества инцидентов, соответствующих данной угрозе, к общему количеству инцидентов. Относительная частота реализации угрозы и результаты обработки инцидентов, соответствующих этой угрозе, позволяют определить актуальность рассматриваемой угрозы

В.3 Идентификация и оценка уязвимостей активов

Идентификация уязвимостей ИБ актуальных активов организации включает определение слабостей в физической среде организации, в автоматизированных системах, аппаратном и программном обеспечении, процедурах, слабостей персонала.

Идентификация уязвимостей ИБ активов осуществляется на основе результатов обработки инцидентов ИБ. В процессе идентификации уязвимостей активов для каждого актива определяется перечень существующих уязвимостей. Источником данных о существующих уязвимостях являются результаты обработки инцидентов, в которых были определены уязвимости, использованные для реализации угрозы ИБ. Эти данные могут быть дополнены и другими выявленными уязвимостями. Для каждого актива указывается одна или несколько характерных для него уязвимостей. В результате должен быть составлен перечень активов и их уязвимостей.

Оценка уязвимости зависит от наличия угрозы, которая могла бы использовать данную уязвимость для своей реализации, и от существующих защитных мер, направленных на устранение возможности использования уязвимости для реализации угрозы.

В.4 Анализ рисков ИБ

Целью анализа риска ИБ является оценка вероятности инцидента и определение уровня риска.

Анализ риска может быть осуществлен с различной степенью детализации в зависимости от критичности активов, результатов идентификации угроз, уязвимостей и инцидентов.

Для оценки вероятности инцидентов необходимо знать перечень идентифицированных сценариев инцидентов с их последствиями, связанными с активами, оценки возможности реализации угроз и оценки возможности использования уязвимостей, а также перечень всех существующих защитных

мер, их эффективности и состояния реализации и использования (как они снижают уязвимости и как противодействуют угрозам).

Результатом является оценка вероятности (возможности) сценариев инцидентов.

Для определения уровня риска должны быть известны перечень сценариев инцидентов с последствиями и оценкой последствий и вероятности сценариев инцидентов (оцененные количественно или качественно)

Уровень риска определяется исходя из комбинации вероятности сценария инцидентов и оценки его последствий, например, с помощью способа с заранее определенными значениями риска для различных сценариев инцидентов.

Таблица В.1 – Определение уровней последствий

	Возможность угрозы	Низкая			Средняя			Высокая		
	Уровни уязвимостей	Н	С	В	Н	С	В	Н	С	В
Уровень последствий	Низкий	1	2	3	2	3	4	3	4	5
	Средний	2	3	4	3	4	5	4	5	6
	Высокий	3	4	5	4	5	6	5	6	7

Результатом является перечень рисков с установленными значениями их уровней.

В.5 Оценивание рисков ИБ

Цель оценивания рисков - сравнение уровней рисков с критериями оценивания риска и критериями принятия риска для определения приемлемых рисков и рисков для последующей обработки.

Для оценивания риска необходимы перечень рисков со значениями их уровней и установленные в документах организации критерии оценивания риска и критерии принятия риска.

При оценивании рисков сравниваются уровни рисков, полученные при анализе риска, с критериями оценивания риска и критериями принятия риска для принятия решений о дальнейших действиях в отношении рисков, а именно,

какие риски необходимо обрабатывать, каковы приоритеты при обработке рисков.

Результатом является перечень рисков с приоритетами при обработке риска в соответствии с критериями оценивания риска и перечень приемлемых рисков в соответствии с критериями принятия риска.

В.6 Обработка рисков ИБ

Цель обработки рисков ИБ - выбор защитных мер для предотвращения, разделения или снижения рисков, а также определение плана обработки рисков. Для обработки риска необходимы перечень рисков с приоритетами их обработки.

Варианты обработки риска должны выбираться исходя из результатов оценки риска, предполагаемой стоимости реализации этих вариантов и их ожидаемой эффективности.

Варианты обработки риска:

- снижение риска;
- сохранение риска;
- предотвращение риска;
- разделение (перенос) риска.

Четыре варианта обработки риска не являются взаимоисключающими. В отдельных случаях организация может получить значительную выгоду от объединения вариантов, таких, как снижение вероятности риска, уменьшение последствий и перенос или сохранение любого остаточного риска.

При выборе защитных мер должны быть учтены различные ограничения, такие как, временные, финансовые, технические, социологические, юридические ограничения.

Для разных вариантов обработки риска должно учитываться:

- как риск осознается затрагиваемыми сторонами;

— наиболее подходящие способы обмена информацией с этими сторонами.

После уточнения плана обработки риска необходимо определить остаточные риски. Это включает обновление или повторную операцию оценки риска с учетом ожидаемого эффекта от предполагаемой обработки риска. Если остаточные риски по-прежнему не будут удовлетворять критериям принятия риска организации, может возникнуть необходимость в дополнительной итерации обработки риска, прежде чем перейти к принятию риска.

Результатом является план обработки риска и остаточные риски.

Приложение Г
(обязательное)

Оценка основных показателей процессов управления ИБ

Таблица Г.1 – Анкета для оценки основных показателей процесса «Идентификация и определение ценности активов»

Обозначение основного показателя	Основной показатель	Оценка основного показателя			
		Н	Ч	В	П
K_{11}^1	Существуют ли меры и (или) средства, используемые для идентификации и определения ценности активов?				
K_{12}^1	Достигают ли существующие меры и средства, используемые для идентификации и определения ценности активов, ожидаемого результата?				
K_{13}^1	Реализована ли деятельность по идентификации и определения ценности активов?				
K_{21}^1	Организовано ли обучение принятому в организации процессу идентификации и определения ценности активов и информируются ли сотрудники об этих процессах?				
K_{22}^1	Достигает ли идентификация и определение ценности активов ожидаемых результатов?				
K_{23}^1	Определен ли перечень нормативных документов организации, регулирующих идентификацию и определение ценности активов?				
K_{31}^1	Зафиксирован ли документально процесс идентификации и определения ценности активов?				
K_{32}^1	Существует ли в организации ролевая политика в области ИБ?				
K_{33}^1	Определены ли цели осуществления процесса идентификации и определения ценности активов?				
K_{34}^1	Определены ли ответственности и полномочия по осуществлению				

Обозначение основного показателя	Основной показатель	Оценка основного показателя			
		Н	Ч	В	П
	идентификации и определения ценности активов?				
K_{35}^1	Идентифицированы ли ресурсы и информация, необходимая для осуществления процесса идентификации и определения ценности активов?				
K_{36}^1	Определен ли перечень результатов (выходов) процесса идентификации и определения ценности активов?				
K_{37}^1	Формализована ли существующая в организации практика в области управления ИБ в виде процедур процесса идентификации и определения ценности активов?				
K_{38}^1	Регламентирован ли в организации подход к обучению и информированию о реализованном процессе идентификации и определения ценности активов?				
K_{39}^1	Установлены ли в организации требования по осуществлению контроля за реализацией процесса идентификации и определения ценности активов?				
K_{310}^1	Осуществляется ли в организации оценка процесса идентификации и определения ценности активов?				
K_{41}^1	Установлена ли (документально зафиксирована) в организации ответственность за процесс идентификации и определения ценности активов (распределены роли по обеспечению ИБ, назначены исполнители ролей и т.п.)?				
K_{42}^1	Доведены ли ответственность и полномочия по осуществлению процесса идентификации и определения ценности активов до сведения ответственных лиц в организации?				
K_{43}^1	Компетентен ли персонал, осуществляющий процесс идентификации и определения ценности активов?				
K_{44}^1	Регламентирован ли в организации процесс идентификации и определения ценности активов?				

Обозначение основного показателя	Основной показатель	Оценка основного показателя			
		Н	Ч	В	П
K_{45}^1	Существует ли в организации контроль за исполнением требований всех нормативных документов организации и нормативных документов внешних регулирующих и надзорных органов в области ИБ?				
K_{46}^1	Соответствует ли процесс идентификации и определения ценности активов общепринятой практике?				
K_{47}^1	Доступны ли ресурсы и информация, необходимая для осуществления процесса идентификации и определения ценности активов?				
K_{48}^1	Определены ли соответствующие методы для проведения измерения (оценки) процесса идентификации и определения ценности активов?				
K_{49}^1	Реализован ли постоянный контроль за реализацией процесса идентификации и определения ценности активов?				
K_{410}^1	Существует ли возможность принятия мер в случае, если процесс идентификации и определения ценности активов неэффективен?				
K_{411}^1	Осуществляется ли совершенствование процесса идентификации и определения ценности активов регламентированным образом?				
K_{51}^1	Определены ли цели улучшения идентификации и определения ценности активов, которые обеспечивают достижение целей деятельности организации?				
K_{52}^1	Идентифицированы ли возможности улучшений, связанные с новыми технологиями?				
K_{53}^1	Направлено ли непрерывное совершенствование ИБ на совершенствование идентификации и определения ценности активов?				

Таблица Г.2 – Анкета для оценки основных показателей процесса «Идентификация и оценка угроз ИБ»

Обозначение основного показателя	Основной показатель	Оценка основного показателя			
		Н	Ч	В	П
K_{11}^2	Существуют ли меры и (или) средства, используемые для идентификации и оценки угроз ИБ?				
K_{12}^2	Достигают ли существующие меры и средства, используемые для идентификации и оценки угроз ИБ, ожидаемого результата?				
K_{13}^2	Реализована ли деятельность по идентификации и оценки угроз ИБ?				
K_{21}^2	Организовано ли обучение принятому в организации процессу идентификации и оценки угроз ИБ и информируются ли сотрудники об этих процессах?				
K_{22}^2	Достигает ли идентификация и оценка угроз ИБ ожидаемых результатов?				
K_{23}^2	Определен ли перечень нормативных документов организации, регулирующих идентификацию и оценку угроз ИБ?				
K_{31}^2	Зафиксирован ли документально процесс идентификации и оценки угроз ИБ?				
K_{32}^2	Существует ли в организации ролевая политика в области ИБ?				
K_{33}^2	Определены ли цели осуществления процесса идентификации и оценки угроз ИБ?				
K_{34}^2	Определены ли ответственности и полномочия по осуществлению идентификации и оценки угроз ИБ?				
K_{35}^2	Идентифицированы ли ресурсы и информация, необходимая для осуществления процесса идентификации и оценки угроз ИБ?				
K_{36}^2	Определен ли перечень результатов (выходов) процесса идентификации и оценки угроз ИБ?				
K_{37}^2	Формализована ли существующая в организации практика в области управления ИБ в виде процедур процесса идентификации и оценки угроз ИБ?				

Обозначение основного показателя	Основной показатель	Оценка основного показателя			
		Н	Ч	В	П
K_{38}^2	Регламентирован ли в организации подход к обучению и информированию о реализованном процессе идентификации и оценки угроз ИБ?				
K_{39}^2	Установлены ли в организации требования по осуществлению контроля за реализацией процесса идентификации и оценки угроз ИБ?				
K_{310}^2	Осуществляется ли в организации оценка процесса идентификации и оценки угроз ИБ?				
K_{41}^2	Установлена ли (документально зафиксирована) в организации ответственность за процесс идентификации и оценки угроз ИБ (распределены роли по обеспечению ИБ, назначены исполнители ролей и т.п.)?				
K_{42}^2	Доведены ли ответственность и полномочия по осуществлению процесса идентификации и оценки угроз ИБ до сведения ответственных лиц в организации?				
K_{43}^2	Компетентен ли персонал, осуществляющий процесс идентификации и оценки угроз ИБ?				
K_{44}^2	Регламентирован ли в организации процесс идентификации и оценки угроз ИБ?				
K_{45}^2	Существует ли в организации контроль за исполнением требований всех нормативных документов организации и нормативных документов внешних регулирующих и надзорных органов в области ИБ?				
K_{46}^2	Соответствует ли процесс идентификации и оценки угроз ИБ общепринятой практике?				
K_{47}^2	Доступны ли ресурсы и информация, необходимая для осуществления процесса идентификации и оценки угроз ИБ?				
K_{48}^2	Определены ли соответствующие методы для проведения измерения (оценки) процесса идентификации и оценки угроз ИБ?				
K_{49}^2	Реализован ли постоянный контроль за реализацией процесса идентификации и оценки угроз ИБ?				
	Существует ли возможность принятия мер в				

Обозначение основного показателя	Основной показатель	Оценка основного показателя			
		Н	Ч	В	П
K_{410}^2	случае, если процесс идентификации и оценки угроз ИБ неэффективен?				
K_{411}^2	Осуществляется ли совершенствование процесса идентификации и оценки угроз ИБ регламентированным образом?				
K_{51}^2	Определены ли цели улучшения идентификации и оценки угроз ИБ, которые обеспечивают достижение целей деятельности организации?				
K_{52}^2	Идентифицированы ли возможности улучшений, связанные с новыми технологиями?				
K_{53}^2	Направлено ли непрерывное совершенствование ИБ на совершенствование идентификации и оценки угроз ИБ?				

Таблица Г.3 – Анкета для оценки основных показателей процесса
«Идентификация и оценка уязвимостей активов»

Обозначение основного показателя	Основной показатель	Оценка основного показателя			
		Н	Ч	В	П
K_{11}^3	Существуют ли меры и (или) средства, используемые для идентификации и оценки уязвимостей активов?				
K_{12}^3	Достигают ли существующие меры и средства, используемые для идентификации и оценки уязвимостей активов, ожидаемого результата?				
K_{13}^3	Реализована ли деятельность по идентификации и оценки уязвимостей активов?				
K_{21}^3	Организовано ли обучение принятому в организации процессу идентификации и оценки уязвимостей активов и информируются ли сотрудники об этих процессах?				
K_{22}^3	Достигает ли идентификация и оценка уязвимостей активов ожидаемых результатов?				
K_{23}^3	Определен ли перечень нормативных документов организации, регулирующих идентификации и оценки уязвимостей активов?				
K_{31}^3	Зафиксирован ли документально процесс идентификации и оценки уязвимостей активов?				
K_{32}^3	Существует ли в организации ролевая политика в области ИБ?				
K_{33}^3	Определены ли цели осуществления процесса идентификации и оценки уязвимостей активов?				
K_{34}^3	Определены ли ответственности и полномочия по осуществлению идентификации и оценки уязвимостей активов?				
K_{35}^3	Идентифицированы ли ресурсы и информация, необходимая для осуществления процесса идентификации и				

Обозначение основного показателя	Основной показатель	Оценка основного показателя			
		Н	Ч	В	П
	оценки уязвимостей активов?				
K_{36}^3	Определен ли перечень результатов (выходов) процесса идентификации и оценки уязвимостей активов?				
K_{37}^3	Формализована ли существующая в организации практика в области управления ИБ в виде процедур процесса идентификации и оценки уязвимостей активов?				
K_{38}^3	Регламентирован ли в организации подход к обучению и информированию о реализованном процессе идентификации и оценки уязвимостей активов?				
K_{39}^3	Установлены ли в организации требования по осуществлению контроля за реализацией процесса идентификации и оценки уязвимостей активов?				
K_{310}^3	Осуществляется ли в организации оценка процесса идентификации и оценки уязвимостей активов?				
K_{41}^3	Установлена ли (документально зафиксирована) в организации ответственность за процесс идентификации и оценки уязвимостей активов (распределены роли по обеспечению ИБ, назначены исполнители ролей и т.п.)?				
K_{42}^3	Доведены ли ответственность и полномочия по осуществлению процесса идентификации и оценки уязвимостей активов до сведения ответственных лиц в организации?				
K_{43}^3	Компетентен ли персонал, осуществляющий процесс идентификации и оценки уязвимостей активов?				
K_{44}^3	Регламентирован ли в организации процесс идентификации и оценки уязвимостей активов?				
K_{45}^3	Существует ли в организации контроль за исполнением требований всех нормативных документов организации и нормативных документов внешних регулирующих и надзорных органов в области ИБ?				

Обозначение основного показателя	Основной показатель	Оценка основного показателя			
		Н	Ч	В	П
K_{46}^3	Соответствует ли процесс идентификации и оценки уязвимостей активов общепринятой практике?				
K_{47}^3	Доступны ли ресурсы и информация, необходимая для осуществления процесса идентификации и оценки уязвимостей активов?				
K_{48}^3	Определены ли соответствующие методы для проведения измерения (оценки) процесса идентификации и оценки уязвимостей активов?				
K_{49}^3	Реализован ли постоянный контроль за реализацией процесса идентификации и оценки уязвимостей активов?				
K_{410}^3	Существует ли возможность принятия мер в случае, если процесс идентификации и оценки уязвимостей активов неэффективен?				
K_{411}^3	Осуществляется ли совершенствование процесса идентификации и оценки уязвимостей активов регламентированным образом?				
K_{51}^3	Определены ли цели улучшения идентификации и оценки уязвимостей активов, которые обеспечивают достижение целей деятельности организации?				
K_{52}^3	Идентифицированы ли возможности улучшений, связанные с новыми технологиями?				
K_{53}^3	Направлено ли непрерывное совершенствование ИБ на совершенствование идентификации и оценки уязвимостей активов?				

Таблица Г.4 – Анкета для оценки основных показателей процесса «Анализ рисков ИБ»

Обозначение основного показателя	Основной показатель	Оценка основного показателя			
		Н	Ч	В	П
K_{11}^4	Существуют ли меры и (или) средства, используемые для анализа рисков ИБ?				
K_{12}^4	Достигают ли существующие меры и средства, используемые для анализа рисков ИБ, ожидаемого результата?				
K_{13}^4	Реализована ли деятельность по анализу рисков ИБ?				
K_{21}^4	Организовано ли обучение принятому в организации процессу анализа рисков ИБ и информируются ли сотрудники об этих процессах?				
K_{22}^4	Достигает ли анализ рисков ИБ ожидаемых результатов?				
K_{23}^4	Определен ли перечень нормативных документов организации, регулирующих процесс анализа рисков ИБ?				
K_{31}^4	Зафиксирован ли документально процесс анализа рисков ИБ?				
K_{32}^4	Существует ли в организации ролевая политика в области ИБ?				
K_{33}^4	Определены ли цели осуществления процесса анализа рисков ИБ?				
K_{34}^4	Определены ли ответственности и полномочия по осуществлению анализа рисков ИБ?				
K_{35}^4	Идентифицированы ли ресурсы и информация, необходимая для осуществления процесса анализа рисков ИБ?				
K_{36}^4	Определен ли перечень результатов (выходов) процесса анализа рисков ИБ?				
K_{37}^4	Формализована ли существующая в организации практика в области управления ИБ в виде процедур анализа рисков ИБ?				
K_{38}^4	Регламентирован ли в организации подход к обучению и информированию о				

Обозначение основного показателя	Основной показатель	Оценка основного показателя			
		Н	Ч	В	П
	реализованном процессе анализа рисков ИБ?				
K_{39}^4	Установлены ли в организации требования по осуществлению контроля за реализацией процесса анализа рисков ИБ?				
K_{310}^4	Осуществляется ли в организации оценка процесса анализа рисков ИБ?				
K_{41}^4	Установлена ли (документально зафиксирована) в организации ответственность за процесс анализа рисков ИБ (распределены роли по обеспечению ИБ, назначены исполнители ролей и т.п.)?				
K_{42}^4	Доведены ли ответственность и полномочия по осуществлению процесса анализа рисков ИБ до сведения ответственных лиц в организации?				
K_{43}^4	Компетентен ли персонал, осуществляющий процесс анализа рисков ИБ?				
K_{44}^4	Регламентирован ли в организации процесс анализа рисков ИБ?				
K_{45}^4	Существует ли в организации контроль за исполнением требований всех нормативных документов организации и нормативных документов внешних регулирующих и надзорных органов в области ИБ?				
K_{46}^4	Соответствует ли процесс анализа рисков ИБ общепринятой практике?				
K_{47}^4	Доступны ли ресурсы и информация, необходимая для осуществления процесса анализа рисков ИБ?				
K_{48}^4	Определены ли соответствующие методы для проведения измерения (оценки) процесса анализа рисков ИБ?				
K_{49}^4	Реализован ли постоянный контроль за реализацией процесса анализа рисков ИБ?				
K_{410}^4	Существует ли возможность принятия мер в случае, если процесс анализа рисков ИБ неэффективен?				
K_{411}^4	Осуществляется ли совершенствование процесса анализа рисков ИБ				

Обозначение основного показателя	Основной показатель	Оценка основного показателя			
		Н	Ч	В	П
	регламентированным образом?				
K_{51}^4	Определены ли цели улучшения анализа рисков ИБ, которые обеспечивают достижение целей деятельности организации?				
K_{52}^4	Идентифицированы ли возможности улучшений, связанные с новыми технологиями?				
K_{53}^4	Направлено ли непрерывное совершенствование ИБ на совершенствование анализа рисков ИБ?				

Таблица Г.5 – Анкета для оценки основных показателей процесса «Оценивание рисков ИБ»

Обозначение основного показателя	Основной показатель	Оценка основного показателя			
		Н	Ч	В	П
K_{11}^5	Существуют ли меры и (или) средства, используемые для оценивания рисков ИБ?				
K_{12}^5	Достигают ли существующие меры и средства, используемые для оценивания рисков ИБ, ожидаемого результата?				
K_{13}^5	Реализована ли деятельность по оцениванию рисков ИБ?				
K_{21}^5	Организовано ли обучение принятому в организации процессу оценивания рисков ИБ и информируются ли сотрудники об этих процессах?				
K_{22}^5	Достигает ли оценивание рисков ИБ ожидаемых результатов?				
K_{23}^5	Определен ли перечень нормативных документов организации, регулирующих процесс оценивания рисков ИБ?				
K_{31}^5	Зафиксирован ли документально процесс оценивания рисков ИБ?				
K_{32}^5	Существует ли в организации ролевая политика в области ИБ?				
K_{33}^5	Определены ли цели осуществления процесса оценивания рисков ИБ?				
K_{34}^5	Определены ли ответственности и полномочия по осуществлению оценивания рисков ИБ?				
K_{35}^5	Идентифицированы ли ресурсы и информация, необходимая для осуществления процесса оценивания рисков ИБ?				
K_{36}^5	Определен ли перечень результатов (выходов) процесса оценивания рисков ИБ?				
K_{37}^5	Формализована ли существующая в организации практика в области управления ИБ в виде процедур оценивания рисков ИБ?				
	Регламентирован ли в организации подход к				

Обозначение основного показателя	Основной показатель	Оценка основного показателя			
		Н	Ч	В	П
K_{38}^5	обучению и информированию о реализованном процессе оценивания рисков ИБ?				
K_{39}^5	Установлены ли в организации требования по осуществлению контроля за реализацией процесса оценивания рисков ИБ?				
K_{310}^5	Осуществляется ли в организации оценка процесса оценивания рисков ИБ?				
K_{41}^5	Установлена ли (документально зафиксирована) в организации ответственность за процесс оценивания рисков ИБ (распределены роли по обеспечению ИБ, назначены исполнители ролей и т.п.)?				
K_{42}^5	Доведены ли ответственность и полномочия по осуществлению процесса оценивания рисков ИБ до сведения ответственных лиц в организации?				
K_{43}^5	Компетентен ли персонал, осуществляющий процесс оценивания рисков ИБ?				
K_{44}^5	Регламентирован ли в организации процесс оценивания рисков ИБ?				
K_{45}^5	Существует ли в организации контроль за исполнением требований всех нормативных документов организации и нормативных документов внешних регулирующих и надзорных органов в области ИБ?				
K_{46}^5	Соответствует ли процесс оценивания рисков ИБ общепринятой практике?				
K_{47}^5	Доступны ли ресурсы и информация, необходимая для осуществления процесса оценивания рисков ИБ?				
K_{48}^5	Определены ли соответствующие методы для проведения измерения (оценки) процесса оценивания рисков ИБ?				
K_{49}^5	Реализован ли постоянный контроль за реализацией процесса оценивания рисков ИБ?				
	Существует ли возможность принятия мер в				

Обозначение основного показателя	Основной показатель	Оценка основного показателя			
		Н	Ч	В	П
K_{410}^5	случае, если процесс оценивания рисков ИБ неэффективен?				
K_{411}^5	Осуществляется ли совершенствование процесса оценивания рисков ИБ регламентированным образом?				
K_{51}^5	Определены ли цели улучшения оценивания рисков ИБ, которые обеспечивают достижение целей деятельности организации?				
K_{52}^5	Идентифицированы ли возможности улучшений, связанные с новыми технологиями?				
K_{53}^5	Направлено ли непрерывное совершенствование ИБ на совершенствование оценивания рисков ИБ?				

Таблица Г.6 – Анкета для оценки основных показателей процесса «Обработка рисков ИБ»

Обозначение основного показателя	Основной показатель	Оценка основного показателя			
		Н	Ч	В	П
K_{11}^6	Существуют ли меры и (или) средства, используемые для обработки рисков ИБ?				
K_{12}^6	Достигают ли существующие меры и средства, используемые для обработки рисков ИБ, ожидаемого результата?				
K_{13}^6	Реализована ли деятельность по обработке рисков ИБ?				
K_{14}^6	Организовано ли обучение принятому в организации процессу обработки рисков ИБ и информируются ли сотрудники об этих процессах?				
K_{21}^6	Достигает ли обработка рисков ИБ ожидаемых результатов?				
K_{22}^6	Определен ли перечень нормативных документов организации, регулирующих процесс обработки рисков ИБ?				
K_{31}^6	Зафиксирован ли документально процесс обработки рисков ИБ?				
K_{32}^6	Существует ли в организации ролевая политика в области ИБ?				
K_{33}^6	Определены ли цели осуществления процесса обработки рисков ИБ?				
K_{34}^6	Определены ли ответственности и полномочия по осуществлению обработки рисков ИБ?				
K_{35}^6	Идентифицированы ли ресурсы и информация, необходимая для осуществления процесса обработки рисков ИБ?				
K_{66}^6	Определен ли перечень результатов (выходов) процесса обработки рисков ИБ?				
K_{37}^6	Формализована ли существующая в организации практика в области управления ИБ в виде процедур обработки рисков ИБ?				
	Регламентирован ли в организации подход к				

Обозначение основного показателя	Основной показатель	Оценка основного показателя			
		Н	Ч	В	П
K_{38}^6	обучению и информированию о реализованном процессе обработки рисков ИБ?				
K_{39}^6	Установлены ли в организации требования по осуществлению контроля за реализацией процесса обработки рисков ИБ?				
K_{310}^6	Осуществляется ли в организации оценка процесса обработки рисков ИБ?				
K_{41}^6	Установлена ли (документально зафиксирована) в организации ответственность за процесс обработки рисков ИБ (распределены роли по обеспечению ИБ, назначены исполнители ролей и т.п.)?				
K_{42}^6	Доведены ли ответственность и полномочия по осуществлению процесса обработки рисков ИБ до сведения ответственных лиц в организации?				
K_{43}^6	Компетентен ли персонал, осуществляющий процесс обработки рисков ИБ?				
K_{44}^6	Регламентирован ли в организации процесс обработки рисков ИБ?				
K_{45}^6	Существует ли в организации контроль за исполнением требований всех нормативных документов организации и нормативных документов внешних регулирующих и надзорных органов в области ИБ?				
K_{46}^6	Соответствует ли процесс обработки рисков ИБ общепринятой практике?				
K_{47}^6	Доступны ли ресурсы и информация, необходимая для осуществления процесса обработки рисков ИБ?				
K_{48}^6	Определены ли соответствующие методы для проведения измерения (оценки) процесса обработки рисков ИБ?				
K_{49}^6	Реализован ли постоянный контроль за реализацией процесса обработки рисков ИБ?				
K_{410}^6	Существует ли возможность принятия мер в случае, если процесс обработки рисков ИБ неэффективен?				

Обозначение основного показателя	Основной показатель	Оценка основного показателя			
		Н	Ч	В	П
K_{411}^6	Осуществляется ли совершенствование процесса обработки рисков ИБ регламентированным образом?				
K_{51}^6	Определены ли цели улучшения обработки рисков ИБ, которые обеспечивают достижение целей деятельности организации?				
K_{52}^6	Идентифицированы ли возможности улучшений, связанные с новыми технологиями?				
K_{53}^6	Направлено ли непрерывное совершенствование ИБ на совершенствование обработки рисков ИБ?				