АННОТАЦИЯ

Пояснительная записка содержит 81 страницу, 8 рисунков, 8 таблиц, 4 приложения, 20 источников.

КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, УГРОЗЫ БЕЗОПАСНОСТИ, ОБЪЕКТ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ, СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ.

Работа посвящена исследованию вопроса обеспечения информационной безопасности медицинского центра как объекта критической информационной инфраструктуры областного центра.

Объектом исследования является информационная инфраструктура медицинского учреждения как составляющая критической информационной инфраструктуры областного центра.

Предметом исследования является комплексная система защиты медицинского учреждения.

Цель настоящей работы заключается в повышении защищенности критических информационных инфраструктур посредством совершенствования комплексной системы защиты медицинского учреждения областного центра.

Практическая значимость работы заключается в том, что ее результаты могут быть использованы государственными и коммерческими организациями для проектирования современных комплексных систем защиты информации, учитывающих требования закона № 187-ФЗ, а также других нормативных документов в отношении обработки данных на субъектах критической информационной инфраструктуры.

СОДЕРЖАНИЕ

ЗАКЛЮЧЕНИЕ

В данной работе было проведено исследование вопроса обеспечения информационной безопасности критической информационной инфраструктуры, на основании которого можно сделать вывод о широком перечне уязвимостей и угроз информационной безопасности применительно к медицинским учреждениям. В работе были проанализированы ключевые аспекты ФЗ № 187 и определены принципы обеспечения безопасности критической информационной инфраструктуры, на основании чего был сделан вывод о необходимости повышения защищенности критических информационных инфраструктур, в частности медицинского учреждения.

Вместе с тем в работе были выявлены критические процессы, определены объекты критической информационной инфраструктуры медицинского учреждения, проведена оценка факторов активности потенциального злоумышленника, а также разработана модель угроз безопасности объектов критической инфраструктуры медицинского учреждения. По результату проведенного анализа была проведена оценка категорий значимых объектов критической информационной инфраструктуры медицинского учреждения в соответствие с Постановлением Правительства РФ № 127 от 8 февраля 2018 г.

На основании проведенного категорирования и приказа № 239 от 25 декабря 2017 "Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации" были выработаны конкретные организационно-технические требования по защите объектов критической информационной инфраструктуры.

В то же время были сформулированы программно-аппаратные направления защиты значимых объектов критической информационной инфраструктуры медицинского учреждения 3 категории. В результате работы

были исследованы организационно-правовое и инженерно-техническое направления защиты, подобраны меры защиты информации в целях нейтрализации угроз, определенных во второй главе, а также построены схемы размещения средств защиты информации.

Полученные результаты могут быть использованы государственными и коммерческими организациями для проектирования современных комплексных систем защиты информации, учитывающих требования закона № 187-ФЗ, а также других нормативных документов в отношении обработки данных на субъектах критической информационной инфраструктуры.

СПИСОК ЛИТЕРАТУРЫ

1. Методика определения угроз безопасности информации в информационных системах // [Электронный ресурс] Режим доступа: https://fstec.ru/component/attachments/download/812 (Дата обращения: 25.11.2018).
2. Банк данных угроз безопасности информации// [Электронный ресурс], Режим доступа: http://bdu.fstec.ru/ (Дата обращения: 25.11.2018).
3. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». М.: Стандартинформ, 2008.
4. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» // [Электронный ресурс], Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=183918 (Дата обращения: 25.11.2018).
5. Жидко Е.А. Информационные риски как аргумент безопасного и устойчивого развития организаций / Е.А. Жидко, Л.Г. Попова // Информация и безопасность, 2010. – №4. – С. 543–552.
6. Кудрявцев А.М. Киберустойчивость информационно-телекоммуникационной сети / М.А. Коцыняк, И.А. Кулешов, А.М. Кудрявцев, О.С. Лаутаи / СПб.: Бостон-спектр, 2015. – 150 с.
7. Постановление Правительства Российской Федерации от 17.02.2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // [Электронный ресурс], Режим доступа: http://www.garant.ru/products/ipo/prime/doc/71783452/ (Дата обращения: 25.11.2018).
8. Постановление Правительства РФ от 8 февраля 2018 г. № 127 “Об утверждении Правил категорирования объектов критической

информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений” // [Электронный ресурс], Режим доступа: http://www.garant.ru/products/ipo/prime/doc/71776120/ (Дата обращения: 25.11.2018).

9. Приказ ФСТЭК от 21.12.2017 №235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» // [Электронный ресурс], Режим доступа: https://fstec.ru/index?id=1606:prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235 (Дата обращения: 25.11.2018).

10. Приказ ФСТЭК от 26.04.2018 №72 «О внесении изменений в регламент ФСТЭК» // [Электронный ресурс], Режим доступа: https://fstec.ru/index?id=1596:prikaz-fstek-rossii-ot-26-aprelya-2018-g-n-72 (Дата обращения: 25.11.2018).

11. Приказ ФСТЭК России ОТ 06.12.2017 N 227 "Об утверждении порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации" // [Электронный ресурс], Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1587-prikaz-fstek-rossii-ot-6-dekabrya-2017-g-n-227 (Дата обращения: 25.11.2018).

12. Приказ ФСТЭК России от 11.12.2017 № 229 «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // [Электронный ресурс], Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1475-prikaz-fstek-rossii-ot-11-dekabrya-2017-g-n-229 (Дата обращения: 25.11.2018).

13. Приказ ФСТЭК России от 22.12.2017 N 236 "Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об

отсутствии необходимости присвоения ему одной из таких категорий" // [Электронный ресурс], Режим доступа: https://fstec.ru/index?id=1607:prikaz-fstek-rossii-ot-22-dekabrya-2017-g-n-236 (Дата обращения: 25.11.2018).

14. Приказом ФСТЭК от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // [Электронный ресурс], Режим доступа: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (Дата обращения: 25.11.2018).

15. Соловьев В.В. Улучшение защищенности распределенной информационной системы персональных данных на основе технологии VPN и терминального доступа // Информационные технологии и проблемы математического моделирования сложных систем. 2017. №18. С. 39-44.

16. Указ Президента Российской Федерации от 25.11.2017 г. № 569 «О внесении изменений в Положение о ФСТЭК» // [Электронный ресурс], Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=183918 (Дата обращения: 25.11.2018).

17. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" // [Электронный ресурс], Режим доступа: http://www.kremlin.ru/acts/bank/42489 (Дата обращения: 25.11.2018).

18. Федеральный Закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» //[Электронный ресурс], Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/ (Дата обращения: 25.11.2018).

19. Федеральный Закон от 27 июля 2006 г. №152-ФЗ «О персональных данных» // [Электронный ресурс], Режим доступа: http://www.consultant.ru/document/Cons_doc_LAW_61801/ (Дата обращения: 25.11.2018).

20. Чукарин А.В. Бизнес-процессы и информационные технологии в управлении современной инфокоммуникационной компанией / А.В. Чукарин. - М.: Альпина Паблишер, 2016. - 512 с.

ПРИЛОЖЕНИЕ А

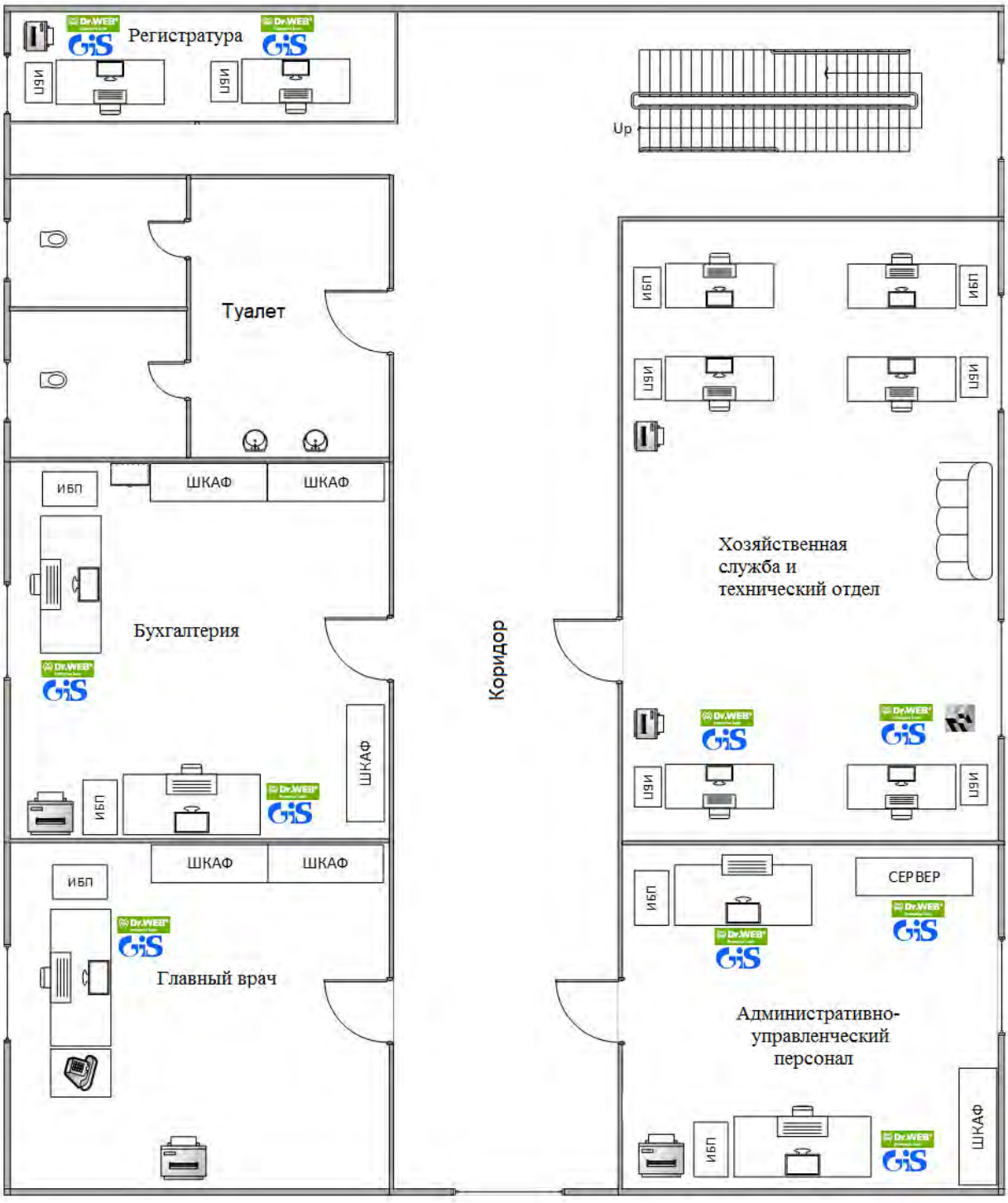

Рисунок А1 – Схема 1-ого этажа медицинского учреждения

Рисунок А2 – Схема 2-5 этажей медицинского учреждения

ПРИЛОЖЕНИЕ Б

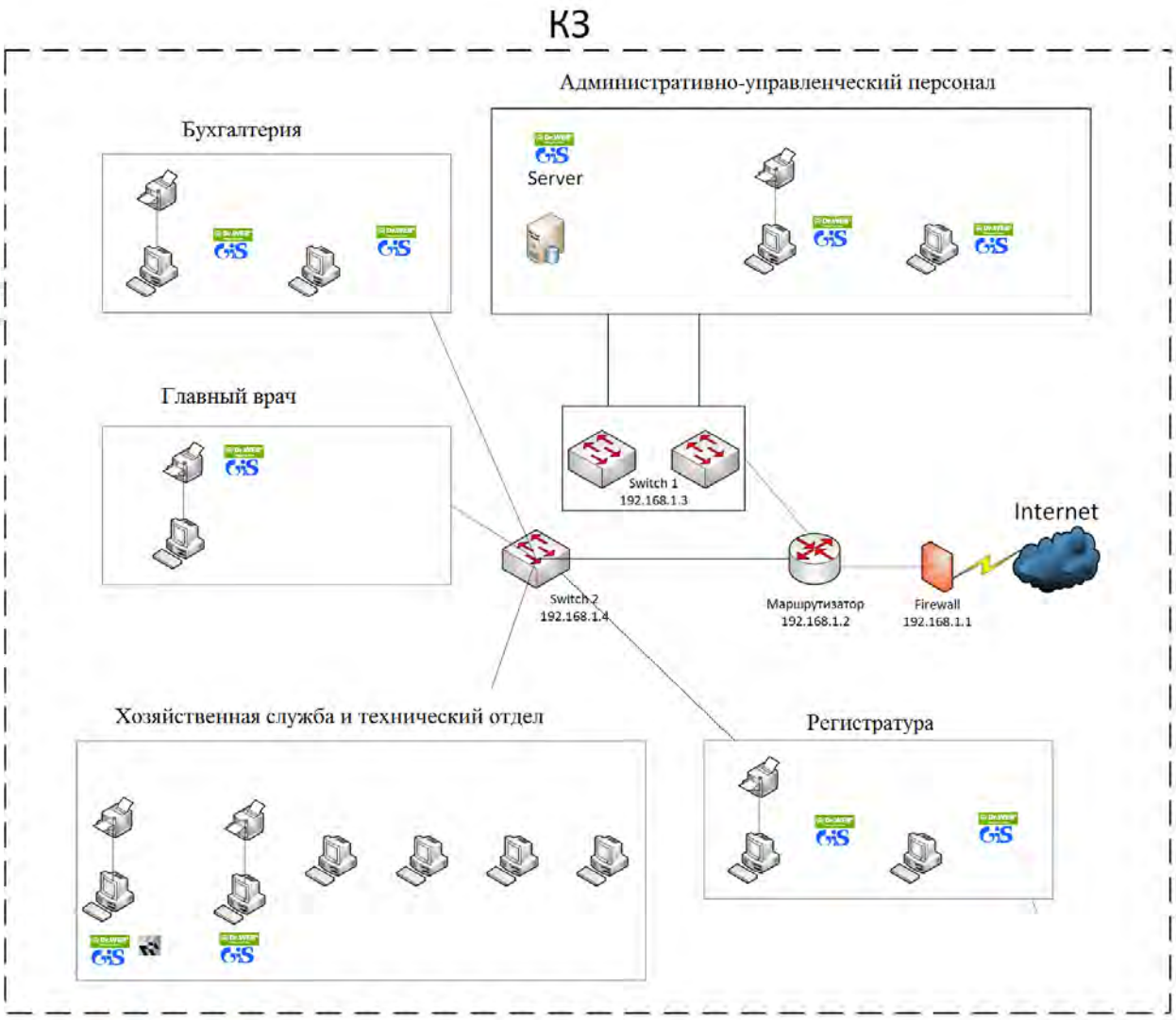

Рисунок Б1 - Топология локальной сети 1-ого этажа медицинского учреждения

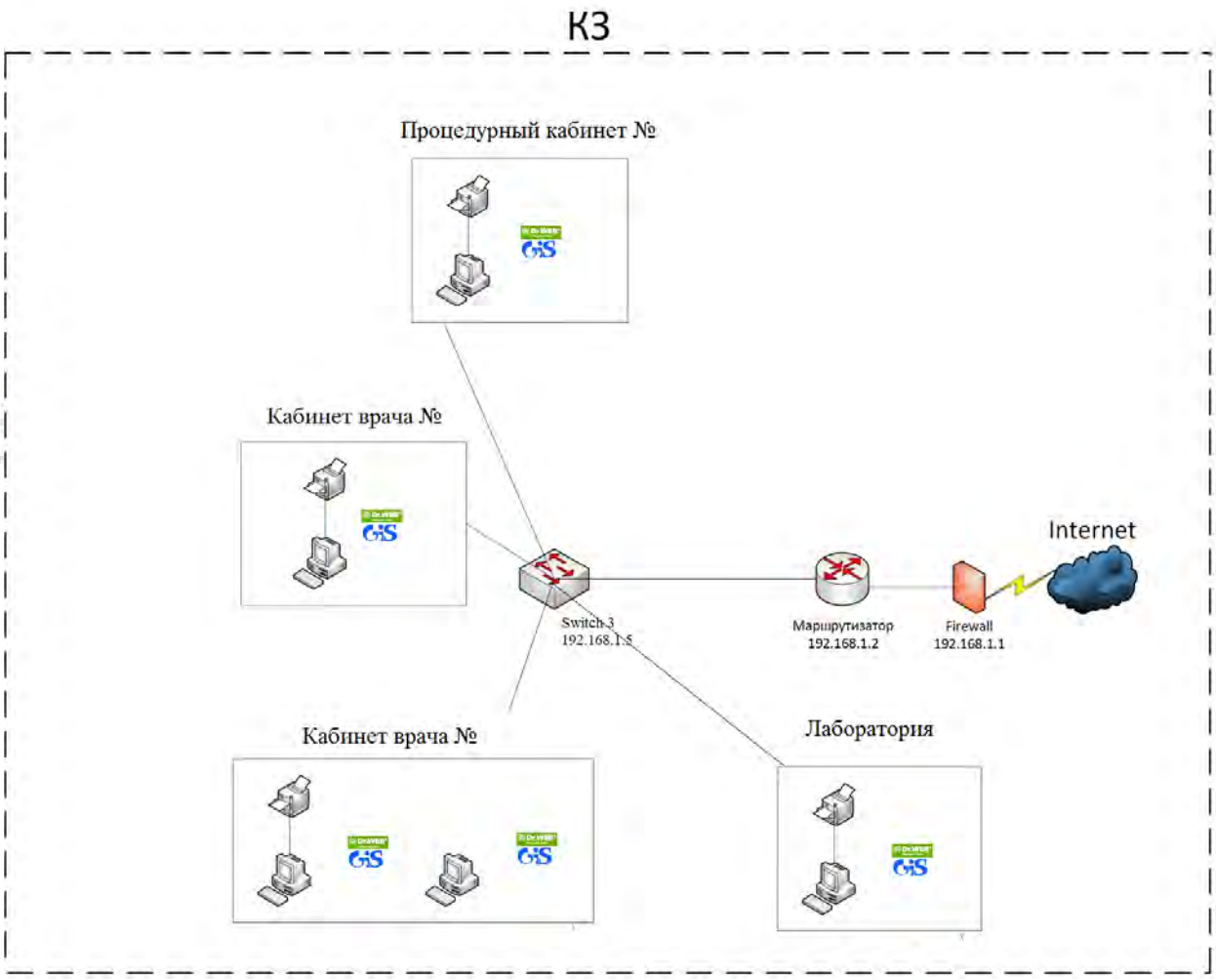

Рисунок Б2 - Топология локальной сети 2-5 этажей медицинского учреждения

ПРИЛОЖЕНИЕ Г

Таблица Г1 – Оценка значимости объектов критической информационной инфраструктуры медицинского учреждения

Показатель		Возможные значения показателя по ПП РФ № 127 от 08.02.2018			ИС, связанные с обслуживанием клиентов	ИС, связанные с обслуживанием сотрудников	АСУ пожаротушением	АСУ оборудованием	Корпоративная сеть
		III категория	II категория	I категория					
I.	Социальная значимость								
1	Причинение ущерба жизни и здоровью людей (человек)	более или равно 1, но менее или равно 50	более 50, но менее или равно 500	более 500	более или равно 1, но менее или равно 50	более или равно 1, но менее или равно 50	более или равно 1, но менее или равно 50	более или равно 1, но менее или равно 50	-
5	Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)	менее или равно 24, но более 12	менее или равно 12, но более 6	менее 6	менее или равно 24, но более 12	менее или равно 24, но более 12	менее или равно 24, но более 12	менее или равно 24, но более 12	-
III	Экономическая значимость								
8	Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, муниципальным унитарным предприятием, государственной компанией, организацией с участием государства и (или) стратегическим	более 5, но менее или равно 10	более 10, но менее или равно 15	более 15	более 5, но менее или равно 10	более 5, но менее или равно 10	более 5, но менее или равно 10	более 5, но менее или равно 10	-

	акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов прогнозируемого объема годового дохода по всем видам деятельности)								
9	Возникновение ущерба бюджетам Российской Федерации, оцениваемого								
а)	В снижении доходов федерального бюджета, (процентов прогнозируемого годового дохода бюджета)	более 0,001, но менее или равно 0,05	более 0,005, но менее или равно 0,1	более 0,1	более 0,001, но менее или равно 0,05	более 0,001, но менее или равно 0,05	более 0,001, но менее или равно 0,05	более 0,001, но менее или равно 0,05	-
б)	В снижении доходов бюджета субъекта Российской Федерации (процентов прогнозируемого годового дохода бюджета)	более 0,001, но менее или равно 0,05	более 0,05, но менее или равно 0,1	более 0,1	более 0,001, но менее или равно 0,05	более 0,001, но менее или равно 0,05	более 0,001, но менее или равно 0,05	более 0,001, но менее или равно 0,05	-
в)	В снижении доходов бюджетов государственных внебюджетных фондов (процентов прогнозируемого годового дохода бюджета)	более 0,01, но менее или равно 0,5	более 0,5, но менее или равно 1	более 1	более 0,01, но менее или равно 0,5	более 0,01, но менее или равно 0,5	более 0,01, но менее или равно 0,5	более 0,01, но менее или равно 0,5	-