«Инфра-Инженерия»

М. В. Тумбинская
М. В. Петровский

ЗАЩИТА ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

УДК 004.056.5
ББК 32.972.5
Т83

Рецензенты:
зав. каф. информационной безопасности ФГБОУ ВО «КНИТУ»
Алехин Александр Дмитриевич;
заместитель генерального директора ООО «АйТи БСА»
Ихсанов Тимур Ринатович

Тумбинская, М. В.

Т83 Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. – Москва ; Вологда : Инфра-Инженерия, 2024. – 144 с. : ил., табл.

ISBN 978-5-9729-1610-8

Рассмотрены основополагающие принципы создания комплексной системы защиты информации на предприятии. Формулируются принципы комплексного обеспечения информационной безопасности на предприятии.

Для студентов высших учебных заведений, обучающихся по направлению подготовки бакалавриата 10.03.01 «Информационная безопасность», профилей подготовки «Организация и технология защиты информации», «Комплексная защита объектов информатизации», специалитета 10.05.02 «Информационная безопасность телекоммуникационных систем». Может быть полезно студентам, обучающимся по техническим специальностям, практикующим специалистам по защите информации, магистрам, аспирантам, докторантам, научным сотрудникам.

УДК 004.056.5
ББК 32.972.5

ISBN 978-5-9729-1610-8

СОДЕРЖАНИЕ

Глава 1. Обзор компьютерных преступлений и злоумышленников. Нормативно-правовая база противодействия компьютерной преступности

§ 1.1. Зарубежный опыт организации службы защиты информации на предприятии

В структуре предприятия, учреждения, организации по зарубежной информации создаются две ключевые позиции, отвечающие за информационную безопасность (ИБ):

− CISO (Chief Information Security Officer), директор по информационной безопасности, которой отвечает за разработку и реализацию политики безопасности компании, адекватной происходящим в ней бизнес-процессам;

− BISO (Business Information Security Officer) менеджер / специалист службы информационной безопасности, который занимается практической реализацией политики ИБ на уровне подразделения, например, планово-экономического отдела, службы маркетинга или автоматизации.

Согласно Gartner Research[1] в компаниях наблюдается несколько тенденций структуры подчиненности специалистов по ИБ в рамках штатного расписания организации. Одна из них вывод CISO из структуры отдела ИТ в подчиненность первому лицу компании (изменение статуса). Другая тенденция (в некоторых компаниях) – слияние департаментов информационной и физической безопасности в связи с тем, что у них есть некоторые общие функции: например, защита перспективных планов развития компании, решение задач контроля и управления доступом, защита активов компании и пр.

Наиболее продвинутые в отношении ИБ и управления рисками компании инвестируют средства в позицию CPO (Chief Privacy Officer), русский аналог заместителя директора по безопасности (только для банков и образовательных учреждений). В этом случае CISO будет подчинен CPO.

Структура подчиненности службы комплексной системы защиты информации предприятия

Можно спрогнозировать, что рынком будут востребованы специалисты по информационной безопасности с мощной технической и управленческой составляющей. К аналогичным выводам пришли аналитики консалтинговой компании KPMG[2], отметив, что в наиболее благополучных с точки зрения информационной безопасности компаниях эта функция входит в компетенцию высшего руководства. Согласно исследованию KPMG, почти в половине организаций ответственность за ИБ была определена на уровне совета директоров, что наиболее характерно для финансового сектора. Непосредственное участие топ-менеджмента организации необходимо для постановки правильных целей в об-

[1] Gartner Customer Strategies & Technologies Summit [Электронный ресурс]: web-портал. – Режим доступа: http://www.gartner.com, свободный – Дата обращения 26.03.2018.

[2] KPMG cutting through complexity [Электронный ресурс]: web-портал. – Режим доступа: http://www.kpmg.com, свободный – Дата обращения 26.03.2018.

ласти ИБ. Руководство должно обеспечить функцию безопасности надлежащим уровнем инвестирования и ресурсов, а также оценивать ее эффективность.

Профиль компетентности. Главная задача CISO это оценка и управление технологическими, производственными и иными рисками компании в срезе информационной безопасности. Роль CISO по этим вопросам предполагает, что данный специалист должен быть способен идентифицировать риски и управлять ими в соответствии с целями и задачами компании, и уровнем ее развития. Свою специфику также вносит сфера деятельности компании, ее размер и стоимость информационных активов. Хороший аналитик и хороший управленец не одно и то же. Это люди с принципиально разным складом ума, структурой мотивации и компетентностью. Для совмещения «двух в одном» профессионала аналитика нужно значительно «подращивать» и укреплять по менеджерской составляющей. Возможно привлечение «готового» или «почти готового» специалиста из числа своих же сотрудников. В этом случае профессиональная компетенция будет усилена еще и знанием конкретного производства.

Сертификация CISO. В настоящее время существуют три наиболее серьезных системы сертификации специалистов по защите информации.

По данным Gartner, среди компаний, предпочтения в области сертификации распределяются следующим образом:

- ✓ сертификацию CISSP (компания ISC) при приеме на работу или аттестации персонала требуют 40 % компаний;
- ✓ сертификат SANS требуют 15 % компаний;
- ✓ другие (MCSE, CISA, ABCP) 25 %.

Функции CISO. По мнению аналитиков, CISO должны быть способны выполнять следующие функции:

- ✓ разработку политики в области ИБ, включая регламенты, стандарты, руководства;
- ✓ разработку принципов классификации информационных потоков и управления ими с точки зрения безопасности;
- ✓ анализ рисков, их оценку;
- ✓ обеспечение персонала всех подразделений руководствами по исполнению политики безопасности, организацию соответствующего обучения и инструктирования;
- ✓ консультирование менеджеров компании и исполнительского персонала в пределах их компетенции по вопросам информационных рисков и защиты от них;
- ✓ согласование всех политик и регламентов для их успешного внедрения на всех уровнях компании;
- ✓ работу в составе рабочих групп или экспертных советов, оценивающих риски при внедрении новых технологий, модернизации производства, формировании планов технического обновления или иных изменениях в бизнесе, включение аспектов ИБ в самые ранние этапы данных проектов;
- ✓ совместная работа со службой безопасности в части, касающейся их обоих, например, в функционировании пропускной системы;

✓ участие вместе с топ-менеджментом в управлении кризисом или внештатной ситуацией в области защиты информации в случае возникновения таковых;

✓ обеспечение высшего менеджмента компании регулярными обзорами состояния информационной безопасности, отчетами о внедрении политики безопасности;

✓ информационную поддержку топ-менеджеров в вопросах изменения законодательства, технических новшеств, имеющих отношение к сфере информационной безопасности.

Предлагается несколько советов, которые могут помочь российским компаниям подготовить своего CISO:

1. С первых дней появления CISO в составе совета директоров ему придется находить общий язык с огромным количеством людей, выполняющих самые разные функции.

2. Открытость, с одной стороны, и избирательные коммуникации, с другой. Позиция предполагает следующую модель поведения: много слушаю, много собираю информации, много синтезирую, мало говорю.

3. Возможно, есть смысл в административном помощнике в связи с высокой информационной загруженностью. Позиция предполагает большую повседневную работу по информированию, разъяснению огромному количеству людей принципов построения системы ИБ и их личной роли в ее нормальном функционировании.

4. CISO не должен бояться слышать регулярное «нет» в ответ на свои предложения и требования, во всяком случае, на первых порах.

5. CISO сам должен быть хорошим менеджером и коммуникатором его работа не может быть выполнена им в одиночку.

Среди международных организаций, принимающих непосредственное участие в борьбе с международной преступностью, особую роль играет Международная организация уголовной полиции (Интерпол). Интерпол – это и механизм, и посредник в практическом сотрудничестве служб уголовной полиции разных государств в их повседневной работе над раскрытием конкретных преступлений, в координации и кооперации предпринимаемых ими совместных усилий. В этом механизме сотрудничества Интерпол действует как единый мировой центр по выработке совместной полицейской стратегии и тактики борьбы с международной организованной преступностью. В 1991 году данный кодификатор был интегрирован в автоматизированную систему поиска и в настоящее время доступен подразделениям Национальных центральных бюро Международной уголовной полиции «Интерпол» более чем 120 стран мира.

Несанкционированный доступ – неправомерный доступ к компьютерной системе или сети путем нарушения охранных мер.

Несанкционированный перехват – неправомерный и осуществленный с помощью технических средств перехват сообщений, приходящих в компьютерную систему или сеть, исходящих из компьютерной системы или сети и передаваемых в рамках компьютерной системы или сети.

Изменение компьютерных данных – неправомерное изменение компьютерных данных.

Компьютерное мошенничество – введение, изменение, стирание или подавление компьютерных данных или компьютерных программ или иное вмешательство в процесс обработки данных, которое влияет на результат обработки данных, что причиняет экономический ущерб или приводит к утрате собственности другого лица, с намерением получить незаконным путем экономическую выгоду для себя или для другого лица.

Компьютерный саботаж – введение, изменение, стирание или подавление компьютерных данных или компьютерных программ, или создание помех компьютерным системам с намерением воспрепятствовать работе компьютера или телекоммуникационной системы.

§ 1.2. Российская нормативно-правовая база в области защиты информации на предприятии

1. Гражданский кодекс Российской Федерации[3].

2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[4].

3. Федеральный закон от 07.07.2003 г. № 126-ФЗ «О связи»[5].

4. Федеральный закон от 04.05.2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»[6].

5. Федеральный закон от 06.04.2011г. № 63-ФЗ «Об электронной подписи»[7].

6. Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне»[8].

7. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»[9].

---

[3] Гражданский кодекс Российской Федерации часть первая от 30 ноября 1994 г. № 51-ФЗ, часть вторая от 26 января 1996 г. № 14-ФЗ, часть третья от 26 ноября 2001 г. № 146-ФЗ и часть четвертая от 18 декабря 2006 г. № 230-ФЗ [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[4] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с последующими изм.) // Собрание законодательства Российской Федерации. – 2006. – № 31 (часть I). – Ст. 3448.

[5] Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи (с последующими изм.) // Собрание законодательства Российской Федерации. – 2003. – № 28. – Ст. 2895.

[6] Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 04.03.2022.

[7] Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[8] Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[9] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

8. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»[10].

9. «Доктрина информационной безопасности Российской Федерации», утверждена Указом Президента Российской Федерации 05.12.2016 г. № 646[11].

10. Указ Президента Российской Федерации от 17.12.1997 г. № 1300 «Концепция национальной безопасности Российской Федерации» в редакции Указа Президента Российской Федерации от 10.01.2000 г. № 24[12].

11. Указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»[13].

12. Указ Президента РФ от 17.04.2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»[14].

13. Постановление Правительства Российской Федерации от 03.11.1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии»[15].

14. Постановление Правительства РФ от 21.11.2011 г. № 957 «Об организации лицензирования отдельных видов деятельности»[16].

---

[10] Указ Президента РФ от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[11] «Доктрина информационной безопасности Российской Федерации», утверждена Указом Президента Российской Федерации 05.12.2016 г. № 646 [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[12] Указ Президента Российской Федерации от 17 декабря 1997 г. № 1300 «Концепция национальной безопасности Российской Федерации» в редакции Указа Президента Российской Федерации от 10 января 2000 г. № 24 [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[13] Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[14] Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[15] Постановление Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии» [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[16] Постановление Правительства РФ от 21 ноября 2011 г. № 957 «Об организации лицензирования отдельных видов деятельности» [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

15. Постановление Правительства РФ от 3.02.2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»[17].

16. Приказ Федеральной службы по техническому и экспортному контролю от 12.07.2012 г. № 84 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации»[18]

17. ГОСТ Р 50922-96. «Защита информации. Основные термины и определения»[19].

18. ГОСТ Р 51275-2006. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»[20].

19. Рекомендации по стандартизации Р 50.1.053-2005. «Информационные технологии. Основные термины и определения в области технической защиты информации»[21].

20. ГОСТ Р 51583-2000. «Порядок создания автоматизированных систем в защищенном исполнении»[22].

21. ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 17 декабря 2008 г. N 430-ст)[23].

---

[17] Постановление Правительства РФ от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[18] Приказ Федеральной службы по техническому и экспортному контролю от 12 июля 2012 г. № 84 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации» [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[19] ГОСТ Р 52551-2006 «Системы охраны и безопасности. Термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 6 июня 2006 г. № 106-ст). [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[20] ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374-ст) [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[21] Рекомендации по стандартизации Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 6 апреля 2005 г. № 77-ст) [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[22] ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»; [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[23] ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 17 декабря 2008 г. № 430-ст) [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

22. ГОСТ 12.1.050-86. «Методы измерения шума на рабочих местах»[24].

23. ГОСТ Р ИСО 7498-2-99. «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации»[25].

24. ГОСТ 2.114-95. «Единая система конструкторской документации. Технические условия»[26].

25. ГОСТ 2.601-2006 «Единая система конструкторской документации. Эксплуатационные документы»[27]

26. ГОСТ 34.201-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»[28].

27. ГОСТ 34.602-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированных систем»[29].

28. ГОСТ 34.003-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»[30].

---

[24] ГОСТ 12.1.050-86 «Система стандартов безопасности труда. Методы измерения шума на рабочих местах» (введен в действие постановлением Госстандарта СССР от 28 марта 1986 г. № 790) (с изменениями и дополнениями) [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[25] ГОСТ Р ИСО 7498-2-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации» (принят и введен в действие постановлением Госстандарта РФ от 18 марта 1999 г. № 77) [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[26] Межгосударственный стандарт ГОСТ 2.114-95 «Единая система конструкторской документации. Технические условия» (утв. постановлением Госстандарта РФ от 8 августа 1995 г. № 425) (с изменениями и дополнениями) [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022. [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[27] ГОСТ 2.601-2006 «Единая система конструкторской документации. Эксплуатационные документы» (введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 22 июня 2006 г. № 118-ст) [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[28] ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» (утв. постановлением Госстандарта СССР от 24 марта 1989 г. № 664) [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[29] ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» (утв. постановлением Госстандарта СССР от 24 марта 1989 г. № 661) [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[30] ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399) [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

29. РД Госстандарта СССР 50-34.698-90. «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов»[31].

30. ГОСТ 34.601-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадия создания»[32].

31. ГОСТ Р 6.30-2003 «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требова-ния к оформлению документов»[33].

32. ГОСТ Р ИСО\МЭК 9126-90. «Информационная технология. Оценка программной продукции. Характеристика качества и руководства по их применению»[34].

33. ГОСТ 2.111-68. «Нормоконтроль»[35].

34. ГОСТ Р 50739-95. «Средства вычислительной техники. Защита от несанкционированного доступа к информации»[36].

35. «Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации», Гостехкомиссия России, Москва, 2002[37].

---

[31] Руководящий документ по стандартизации РД 50-34.698-90 «Методические указания "Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов"» (утв. и введены в действие постановлением Государственного комитета СССР по управлению качеством продукции и стандартами от 27 декабря 1990 г. № 3380) [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[32] ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» (утв. постановлением Госстандарта СССР от 29 декабря 1990 г. № 3469) [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[33] ГОСТ Р 6.30-2003 «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов» [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[34] ГОСТ Р ИСО\МЭК 9126-90 «Информационная технология. Оценка программной продукции. Характеристика качества и руководства по их применению». [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[35] ГОСТ 2.111-68 «Единая система конструкторской документации. Нормоконтроль» (утв. Госстандартом СССР в декабре 1967 г.) (с изменениями и дополнениями) [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[36] ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» (принят постановлением Госстандарта РФ от 9 февраля 1995 г. № 49)

[37] «Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации», Гостехкомиссия России, Москва, 2002[Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

36. «Временная методика оценки защищённости конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации», Гостехкомиссия России, Москва, 2002[38].

37. «Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам», Гостехкомиссия России, Москва, 2002[39].

38. «Временная методика оценки защищенности речевой конфиденциальной информации от утечки за счет электроакустических преобразований в вспомогательных технических средствах и системах», Гостехкомиссия России, М., 2001[40].

39. ГОСТ Р 50949-2001 «Средства отображения информации индивидуального пользования. Методы измерений и оценки эргономических параметров и параметров безопасности»[41].

40. ГОСТ Р 50628-2000 «Совместимость технических средств электромагнитная. Устойчивость машин электронных вычислительных персональных к электромагнитным помехам. Требования и методы испытаний»[42].

41. ГОСТ Р 51319-99. «Совместимость технических средств электромагнитная. Приборы для измерения радиопомех. Технические требования и методы испытаний»[43].

---

[38] «Временная методика оценки защищённости конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации», Гостехкомиссия России, Москва, 2002[Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[39] «Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам», Гостехкомиссия России, Москва, 2002 [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[40] «Временная методика оценки защищенности речевой конфиденциальной информации от утечки за счет электроакустических преобразований во вспомогательных технических средствах и системах», Гостехкомиссия России, Москва, 2001 год [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

[41] ГОСТ Р 50949-2001 «Средства отображения информации индивидуального пользования. Методы измерений и оценки эргономических параметров и параметров безопасности» (принят постановлением Госстандарта России от 25 декабря 2001 г. № 576-ст) [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022

[42] ГОСТ Р 50628-2000 «Совместимость технических средств электромагнитная. Устойчивость машин электронных вычислительных персональных к электромагнитным помехам. Требования и методы испытаний» (принят и введен в действие постановлением Госстандарта РФ от 26 декабря 2000 г. № 417-ст) [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022

[43] ГОСТ Р 51319-99 «Совместимость технических средств электромагнитная. Приборы для измерения индустриальных радиопомех. Технические требования и методы испытаний» (принят постановлением Госстандарта РФ от 28 декабря 1999 г. № 795-ст) [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.

42. ГОСТ Р 51320-99. «Совместимость технических средств электромагнитная. Радиопомехи индустриальные. Методы испытаний технических средств – источников индустриальных радиопомех»[44].

43. «Правила устройства электроустановок (ПУЭ)», 7-е изд., М., 2002[45].

44. ГОСТ Р 50922-2006 «Защита информации Основные термины и определения»[46].

45. ГОСТ Р ИСО 7498-1-99. «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель»[47].

46. ГОСТ Р 40.002-2000 «Система сертификации ГОСТ Р. Регистр систем качества. Основные положения)» [48].

47. «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение ПКЗ-2005), приказ ФСБ от 9 февраля 2005 г. № 66 (зарегистрировано в Минюсте Российской Федерации 3 марта 2005 г. № 6382)[49].

48. Указ Президента Российской Федерации 1995 г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации»[50].

---

[44] ГОСТ Р 51320-99 «Совместимость технических средств электромагнитная. Радиопомехи индустриальные. Методы испытаний технических средств – источников индустриальных радиопомех» (введен в действие постановлением Госстандарта РФ от 22 декабря 1999 г. № 655-ст) [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022

[45] «Правила устройства электроустановок (ПУЭ)», [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022

[46] ГОСТ Р 50922-2006 «Защита информации Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст)

[47] ГОСТ Р ИСО/МЭК 7498-1-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель» (принят и введен в действие постановлением Госстандарта РФ от 18 марта 1999 г. № 78) [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022

[48] ГОСТ Р 40.002-2000 «Система сертификации ГОСТ Р. Регистр систем качества. Основные положения» (введен в действие постановлением Госстандарта РФ от 13 апреля 2000 г. № 107-ст) [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022

[49] Приказ ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (с изменениями и дополнениями) [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022

[50] Указ Президента РФ от 3 апреля 1995 *г.* № 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» [Электронный ресурс]: web-портал. – Режим доступа: http://www.garant.ru, свободный – Дата обращения 26.02.2022.