обеспечить высокий уровень контроля оборудования.Технология адаптируема и интегрируема к любой подсистеме [3].

4. Цифровой контроль, управление маршрутом. Суда следуют по заранее заданным маршрутам, но анализируя оперативную морскую и грузовую обстановку, операторы могут наметить оптимальный (не только по времени, но и энергозатратам) маршрут. Предсказать егозаранее часто невозможно.Предупреждения о пиратах, загрузке портатакже важны.

5. Интеллектуальное маневрирование. Важная задача судоходства – внедрение автономного управления, плавания. Интеграция интеллектуальных структур, технологий (искусственный интеллект, глубокое обучение, IoT-маневрирование и др.) позволит судам оставаться на курсе, без постоянного вмешательства.

6. Интегрированные системы. Наблюдение за судовыми подсистемами – сложнейшая задача. Интегрированные управляющие системы позволяют «мониторить» ситуацию на судне и вне его с помощью центрального судового сервера, управляющего и двигателем, и маневрированием, и связью. Если параметры состояния (например, частота вращения двигателя) близки к пороговым, будет соответствующее предупреждение.

7. Блокчейн. Это технология (можно уже говорить о методологии) позволит морскому судоходству воспользоваться высоким качеством, высокой надежностью данных, процессов, smart-контрактами, получая низкие транзакционные издержки, упрощение взаимодействий и др.

8. Робототехника (дроны). Как и везде, передовая робототехника повлияла и на судовождение.Роботы используются в обслуживании, системах безопасности и технического контроля судов. Уже начали заменять людей роботами в опасных условиях, например, при очистке корпусов, удаленном осмотре судов.

Морские дроны используются для доставки на суда, обеспечения безопасности (например, наблюдения), удаленных проверок.3D-печать позволит изготовить нужную деталь по ходу движения на борту судов.

Заключение

Новые технологии позволяют выводить морскую отрасль на высокий уровень. Повышается эффективность судоходства, оно превращается в крупнейшую транспортную инфраструктуру.

Литература

1. Таровик О.В., Топаж А.Г. и др. Моделирование систем арктического морского транспорта: основы междисциплинарного подхода и опыт практических работ // Арктика: экология и экономика.– 2017.– №1.– т.25. – С. 86-101.
2. Choi M., Chung H., Yamaguchi H., et al. Arctic sea route path planning based on an uncertain ice prediction model // Cold Regions Science & Technology, 2015, N109. –pp.61-69.
3. Казиев В.М., Казиева Б.В. Интернет вещей и уязвимость взаимодействий «их» и «нас». Россия, Европа, Азия: цифровизация глобального пространства: Труды III Межд. научно-практич. форума (ноябрь, 2020, Невинномысск) / ред. И.В. Пеньковой. – Ставрополь, 2020.– С. 318-322.
4. Фролов, А. В. BigData и виртуальные ЦОД / А.В. Фролов, А.А. Титова, Е.А. Верещагина // Промышленные АСУ и контроллеры. – 2022. – № 2. – С. 25-29. – DOI 10.25791/asu.2.2022.1347. – EDN AJUXPV.

References

1. Tarovik O.V., Topazh A.G. et al. Modeling of Arctic maritime transport systems: the basis of an interdisciplinary approach and practical experience // Arctic: ecology and economics, 2017, no. 1, vol. 25. - p.86-101.
2. Choi M., Chung H., Yamaguchi H., et al. Arctic sea route path planning based on an uncertain ice prediction model // Cold Regions Science & Technology, 2015, N109. –pp.61-69.
3. Kaziev V.M., Kazieva B.V. The Internet of Things and the Vulnerability of "Them" and "Us" Interactions. Russia, Europe, Asia: digitalization of the global space: Proceedings of the III Int. scientific and practical. Forum (November, 2020, Nevinnomyssk) / ed. I.V. Penkova. -Stavropol, 2020. -p.318-322.
4. Frolov, A. V. Big Data and virtual data centers / A. V. Frolov, A. A. Titova, E. A. Vereshchagina // Industrial ACS and controllers. - 2022. - No. 2. - P. 25-29. – DOI 10.25791/asu.2.2022.1347. – EDN AJUXPV.

УДК 004.023
DOI: 10.34046/aumsuomt104/25

МЕТОДЫ ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ И РАСЧЕТ КИБЕРРИСКОВ

А.В. Лошкарев, аспирант

В статье приведены эффективные научно обоснованные методы обеспечения кибербезопасности, а также расчет киберрисков и их оценка. Все пункты сконструированы грамотно и последовательно. В

статье рассматривается несколько способов расчета киберрисков для выявления наиболее действующего, показаны выведенные формулы расчета рисков, а также потенциального ущерба, что необходимо учитывать при выборе мер и методов в обеспечении информационной безопасности всех баз данных и систем. На примере ряда судов были рассмотрены и доказаны наиболее эффективные методы защиты информационной безопасности. Одним из таких методов по предотвращению кибервзломов является комбинированный метод, что повышает безопасность системы в несколько раз. Приведена формула коэффициента эффективности, которая показывает, что чем больше методов используется для защиты системы, тем выше ее безопасность. В связи с вышеизложенным можно сделать вывод: используя все необходимые эффективные методы по обеспечению информационной безопасности, рекомендации по предотвращению киберпреступлений и выполнив расчет оценки рисков эффективным способом, можно избежать кибервзломы и несанкционированный доступ ко всем важным информационным ресурсам.
Ключевые слова: Информационная безопасность, кибербезопасность, вирус, антивирусная программа, киберриск, кибервзлом, план по кибербезопасности, конфиденциальные информационные данные

CYBER SECURITY METHODS AND CALCULATION OF CYBER RISKS

A. V. Loshkarev

The article presents effective scientifically based methods of ensuring cybersecurity, as well as the calculation of cyber risks and their assessment. All items are designed correctly and consistently. The article discusses several ways of calculating cyber risks to identify the most effective, shows the derived formulas for calculating risks, as well as potential damage, which must be taken into account when choosing measures and methods to ensure information security of all databases and systems. Using the example of a number of courts, the most effective methods of protecting information security were considered and proved. One of these methods to prevent cyber-hacking is the combined method, which increases the security of the system several times. The formula of the efficiency coefficient is given, which shows that the more methods are used to protect the system, the higher its security. In connection with the above, we can conclude: using all the necessary effective methods to ensure information security, recommendations for the prevention of cybercrime and performing a risk assessment calculation in an effective way, it is possible to avoid cyber intrusions and unauthorized access to all important information resources.
Key words: Information security, cyber security, virus, antivirus program, cyber risk, cyber hacking, cyber security plan, confidential informational data

Введение

Надежная и защищенная работа сетей передачи данных, компьютерных систем и мобильных устройств является важнейшим условием для функционирования государства и поддержания экономической стабильности общества. На безопасность работы ключевых информационных систем общего пользования оказывают влияние многие факторы: кибератаки, нарушения, вызванные физическим воздействием, выход из строя программного и аппаратного обеспечения, человеческие ошибки. Перечисленные явления наглядно демонстрируют, насколько современное общество зависит от стабильности работы информационных систем.

На сегодняшний день многие структуры используют системы, основанные на оцифровке, интеграции и автоматизации - это увеличивает риск несанкционированного доступа или злонамеренных атак на системы и сети в несколько раз, впоследствии чего данные могут быть изменены или уничтожены, что влечет за собой различного рода проблемы в работе всей системы в целом.

Реализация мер по защите программ, сетей и систем от цифровых атак, направленных на получения доступа к конфиденциальным данным, расчет и оценка киберрисков, - необходимая составляющая кибербезопасности и является очень непростой задачей.

В статье приведен анализ методов расчета киберрисков и мер по обеспечению информационной безопасности систем.

Расчет киберрисков и их оценка

Кибербезопасноть решает ряд необходимых задач по безопасности систем и различных баз данных. Проводится идентификация информационных ресурсов, определяются уязвимые составляющие системы, составляется список предположительных угроз со стороны киберпреступников и разрабатывается план по кибербезопасности, содержащий расчет киберрисков информационной безопасности и его оценку, что показывает на необходимость принятия разработанных мер и средств защиты от таких видов угроз.

Что такое киберриск?

Киберриск – это возможность использование уязвимостей системы кибератакой для причинения серьезного ущерба различным базам данных [1].

Существуют различные способы расчета киберрисков.

Стандарт NIST 800-30 предлагает использовать формулу расчета значения риска (R) путем

произведения вероятности реализации угрозы (P(t)) и степени влияния угрозы на актив (S) [5]:

$$R = P(t) \times S \quad (1)$$

Этот метод является простым способом вычисления значения киберриска, но рассчитывается в относительных единицах, которые необходимо ранжировать по степени значимости.

Стандарт ГОСТ Р ИСО/МЭК ТО 7 приводит формулу расчета киберриска, отличную от NIST 800-30 с использованием третьего факторы – вероятность наличия уязвимостей (P(V)) [6]:

$$R = P(t) \times P(V) \times S \quad (2)$$

В этом методе вероятности представляют собой шкалу с тремя значениями: низкая, средняя, высокая, а ценность активов – числовое значение от 0 до 4.

Для оценки киберрисков в таком методе расчета необходимо сопоставление количественных значений качественным.

Стандарт BS 7799 предлагает вычислять киберриск по трем показателя: ценность ресурсов (S), уровень угрозы (L(t)), степень уязвимости (L(V)) [7].

$$R = S \times L(t) \times L(V) \quad (3)$$

Значение киберриска варьируется от 0 до 8, в результате чего по каждому активу приводится список предположительных угроз с различными значениями риска.

Несмотря на простую формулу, такой метод является довольно сложным, так как вычисления киберрисков происходит по таблицам позиционирования значений уровня угроз, степени вероятности использования уязвимости и стоимости активов.

Рассмотрев и проанализировав все вышеперечисленные способы расчета киберрисков и ее оценку можно сделать следующий вывод: расчет киберрисков производится с использованием показателей угроз и ценности актива, значения которых рассчитывается в условных единицах, что не дают реального представления уровня риска и размер предполагаемого ущерба в денежном эквиваленте.

Для более точного и надежного расчета киберрисков предлагается разделить процедуру вычисления в два этапа:

1. Расчет значения технического риска
2. Расчет потенциального ущерба

Технический риск состоит из вероятностей реализации угроз и возможного использования уязвимостей системы информационной инфраструктуры, учитывая уровень конфиденциальности, целостности и доступности.

Для расчета технического риска используется три формулы:

1. Формула расчета риска конфиденциальности

$$R_C = k_C \times \mathrm{P(T)} \times \mathrm{P(V)} \quad (4)$$

R_C – значение риска конфиденциальности

k_C – коэффициент конфиденциальности информационной инфраструктуры

P(T) – вероятность реализации угрозы

P(V) – вероятность использования уязвимостей

2. Формула расчета риска целостности

$$R_i = k_i \times \mathrm{P(T)} \times \mathrm{P(V)} \quad (5)$$

R_i – значение риска целостности

k_i – коэффициент целостности информационной инфраструктуры

3. Формула расчета риска доступности

$$R_a = k_a \times \mathrm{P(T)} \times \mathrm{P(V)} \quad (6)$$

R_a – значение риска доступности

k_a – коэффициент доступности информационной инфраструктуры

Такая методика расчета позволяет произвести более детальную и точную оценку киберрисков.

Используя значения рисков конфиденциальности, целостности и доступности, выведем общую формулу технического риска (R):

$$R = \frac{R_c + R_i + R_a}{3} = \frac{P(T) \times P(V) \times (k_c + k_i + k_a)}{3} \quad (7)$$

Получив безразмерное значение вероятности возникновения риска компрометации информационной инфраструктуры, можно вычислить значение потенциального ущерба от кибернападения по формуле (8).

$$D = \mathrm{R} \times S \quad (8)$$

D – значение потенциального ущерба

S – предполагаемые потери (в денежном эквиваленте)

Такая предложенная методика расчета позволяет точно оценить значение киберриска информационной инфраструктуры и получить рассчитанные потери в денежном эквиваленте в случае возникновения информационных уровней угроз безопасности.

Итак, рассмотрев и проанализировав несколько способов расчета киберрисков, можно сделать вывод: для более точной и эффективной оценки значения киберрисков предлагается использовать расчет технического риска с учетом уровней конфиденциальности, доступности и целостности и потенциального ущерба, что дает значение в денежном эквиваленте. По полученным результатам производится анализ, который пока-

зывает на необходимость принятия мер и использования методов по обеспечению информационной безопасности от кибератак.

Методы защиты информационной безопасности

В современном технологическом мире ряд эффективных методов, технологий и процессов являются необходимой составляющей для защиты целостности систем, программ и информационных баз данных от различных кибератак.

Методов по обеспечению информационной безопасности значительное множество, такие как инструктаж, законы по информационной безопасности, запрет на использование нелицензированных переносных носителей, средств и программ, пароли, камеры видеонаблюдения, межсетевые экраны, антивирусные программы, резервное копирование, системы шифрования, замки, сейфы, ограничение доступа к средствам информации, системы сканирования и многое другое.

Все методы обеспечения информационной безопасности можно классифицировать на технические, административные, физические, правовое и комбинированные (как показано на рисунке 1) [2, 3, 4].

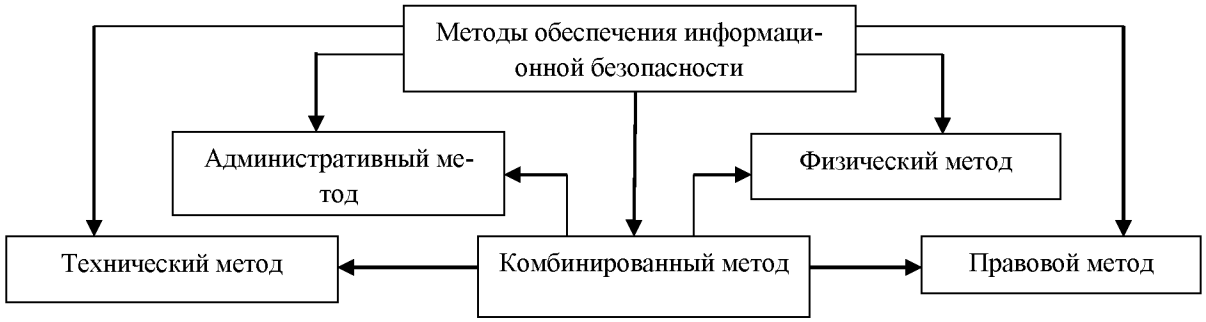

Рисунок 1 - Классификация методов обеспечения информационной безопасности

Каждый из методов обеспечения информационной безопасности в своем роде является эффективным способом защиты. Но многие из них имеют значительные недостатки в использовании.

Рассмотрим каждый метод обеспечения информационной безопасности на примере ряда судов трех разных судоходных компаний (Компания №1 «Jungerhans», суда «Hercules J», «Regina J»; Компания №2 «MOL», суда «Emerald Ace», «APL Poland»; Компания №3 «Interscan», суда «Challenger», «Patriot», «Christina»).

- Административный метод – способ теоретической защиты информации в практическом применении.

Примером административного метода является запрет на использование собственной техники, инструктаж, ограничение доступа к средствам информации. Все эти методы используются на каждом из судов всех трех рассматриваемых компаний. Они имеют значительный недостаток: человеческий фактор. Трудно проследить исполнение этих методов всеми членами экипажа, что повышает риск возникновение угроз.

Также к этой классификации можно отнести резервное копирование. По сравнению с другими административными способами защиты информации этот метод является надежным средством в обеспечение сохранности информационных баз данных. На каждом судне всех трех компаний имеются специальные USB-носители, где хранится вся необходимая информация в случае ее утери, киберсбоев или действующих киберугроз (рисунок 2).

- Правовой метод – способ защиты информации путем ужесточения мер наказания за киберпреступления.

К правовому методу относится ужесточение наказаний за киберпреступления в области информационной безопасности, а также обязательное лицензирование деятельности в этом направлении.

Непременно, данный метод необходим в области кибербезопасности, но в масштабах значительных киберпреступлений со значительными наказаниями. Недостаток: для предъявления наказания необходим киберпреступник, но не всегда расследование имеет положительный эффект. На судах данный метод не применяется.

- Физический метод – это такой метод, который можно назвать физической охраной не только информационных баз, но и средств, содержащих конфиденциальные информационные ячейки.

Рисунок 2 - USB-носители с резервной базой данных судна «Challenger»

К охранной системе можно отнести замки, сейфы, камеры видеонаблюдения, отпечаток пальца, сканирование сетчатки глаза и многое другое. Такой метод позволяет сохранять данные на носителях и дает доступ только одобренным организацией людям.

Но все эти способы, кроме сейфов и замков, являются достаточно дорогостоящими и сложны в обслуживании. Как показывает статистика проанализированных судов трех рассматриваемых компаний, на практике такие методы обеспечения информационной безопасности не используются.

- Технический метод – это способ зашиты информационных баз путем разработанных технологий защиты данных и обнаружения киберпреступлений [3].

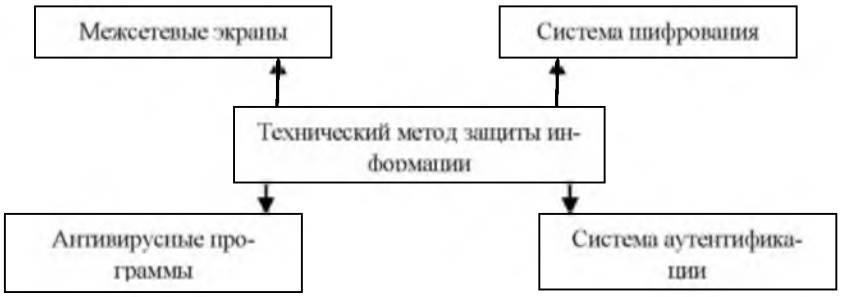

Рисунок 3 - Разработанные технические методы по обеспечению информационной безопасности

К техническому методу обеспечения информационной безопасности можно отнести следующее (как показано на рисунке 3):

1. Межсетевые экраны (МЭ) – это средство обеспечения безопасности внутри сетевой системы, осуществляющее путем применения установленных правил пропускную систему входящего и исходящего сетевого трафика. Недостатками этого способа являются использование дорогостоящих «помощников» МЭ, таких как сервер URL-фильтрации, IPS и другое, низкая пропускная способность, а также недостаточно полный набор функциональных возможностей для защиты систем и различных баз данных. На судах такой метод не применяется.

2. Антивирусная программа – это разработанная специальная программа, предназначенная для обнаружения вирусов и вредоносных программ, а также «лечение» и восстановление зараженных файлов или операционной системы [3, 8]. Использование этого способа защиты повышает уровень кибербезопасности. Но необходимо постоянно контролировать и обновлять программу. На всех судах используются антивирусные программы (рисунок 4).

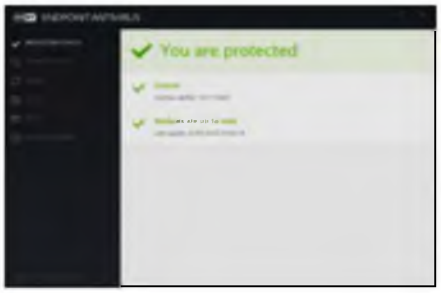

Рисунок 4 - Антивирусная программа, используемая на судне «Emerald Ace»

3. Система аутентификации – способ защиты информационных данных путем использования паролей для безопасности систем [3, 8].

Этот метод является надежным и эффективным способом в обеспечении безопасности.

Вероятность подбора пароля можно рассчитать по формуле (9) через скорость подбора пароля (V), период действия пароля (T) и числа всевозможных паролей (N).

$$P = \frac{V \times T}{N} \quad (9)$$

В свою очередь, число всевозможных паролей (10) рассчитывается произведением числа символов алфавита (S) и длины выбранного пароля (L).

$$N = S \times L \quad (10)$$

Таким образом, общая формула вероятности подбора пароля выглядит следующим образом:

$$P = \frac{V \times T}{S \times L} \quad (11)$$

Из общей выведенной формулы вероятности подбора пароля можно сделать следующий вывод: на стойкость и эффективность пароля влияет частота его смены.

На каждом из судов всех трех компаний используется система аутентификации, и смена паролей всех систем осуществляется в соответствии с требованиями компаний.

4. Система шифрования – это преобразование информационных данных путем специального алгоритма с целью сокрытия их от неавторизированных лиц. Алгоритмом любого шифрования является использование специального ключа, который дает доступ к преобразованию информации в этом алгоритме [1]. Преимущественным недостатком этого метода является сложность использования ключа пользователем, а также создание и обслуживание этой инфраструктуры требует значительных денежных затрат. На судах метод шифрования не используется.

Каждый технический способ повышает уровень защиты информационной системы. Но, как и другие классификационные методы, имеют ряд недостатков, что ограничивает пользователя в их использовании. Как показывает анализ, метод аутентификации и антивирусные программы являются довольно простыми и эффективными способами для обеспечения многих направлений в кибербезопасности в отличие от остальных.

- Комплексный метод – это метод, который включает совокупность частично или всех методов обеспечения транспортной безопасности.

Зачастую использование только пары методов недостаточно. Самый надежный и эффективный способ защиты всего комплекса системы – использование множества методов обеспечения информационной безопасности одновременно.

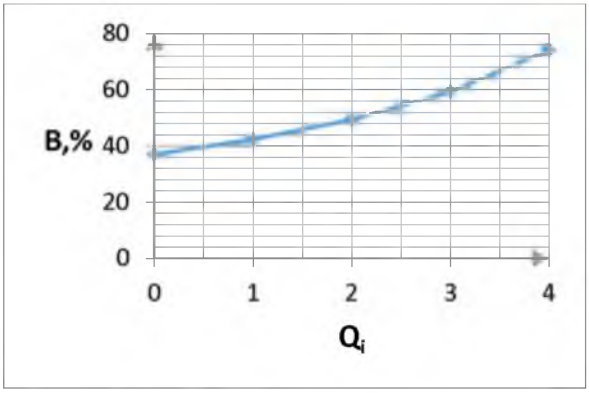

Рисунок 5 - График эффективности защиты систем при использовании методов обеспечения безопасности

На рисунке 5 приведен график эффективной защиты систем от различных кибернападений, в соответствии с формулой (12), который показывает, что коэффициент эффективности использования методов обеспечения информационной безопасности зависит от количества используемых методов одновременно.

$$B,\% = \frac{100}{\frac{1}{2} \times (Q_V + Q_H) \times k} \quad (12)$$

где B – коэффициент эффективности

Q_V – количество всех имеющихся методов обеспечения безопасности

Q_H – количество неиспользуемых методов. Оно зависит от разности всех имеющихся и используемых методов, как показано по формуле (13)

k – коэффициент обтекаемости – это коэффициент, показывающий эффективность системы в единичном соотношении. Среднее значение коэффициента обтекаемости 0,675.

$$Q_H = Q_V - Q_i \quad (13)$$

где Qi – количество используемых методов обеспечения безопасности

Общая формула коэффициента эффективности использования методов безопасности выглядит следующим образом:

$$B = \frac{1}{\frac{1}{2}\times(2Q_V - Q_i)\times k} \quad (14)$$

Таким образом, методы обеспечения информационной безопасности являются главной составляющей в области кибербезопасности. Использование комплексного метода позволяет повысить коэффициент эффективности в несколько раз, что обеспечивает более надежную безопасность информационных баз данных от кибератак.

Рассмотрев и изучив комплекс методов, направленных на обеспечения кибербезопасности, на примере ряда судов трех различных судоходных компаний можно сделать следующий вывод: каждый из методов обеспечения безопасности повышает уровень защиты информационной инфраструктуры. Самыми простыми и надежными способами являются резервное копирование, антивирусные программы, система аутентификации и использование сейфов и замков для сохранности носителей конфиденциальной информации. Эти методы доказали свою эффективность и рекомендованы к применению. А также, используя комплекс методов обеспечения информационной безопасности одновременно, уровень кибербезопасности увеличивается в разы, что уменьшает риск возникновения киберугроз.

Заключение:

В настоящий момент все сферы деятельности, будь это судоходная компания, коммерческая, медицинская, правительственная структура, связаны с электронной системой сбора, обработки и хранения личных конфиденциальных информационных баз данных. Защита всех структур – важная составляющая для поддержания жизнедеятельности нашего общества, ведь в ином случае это может привести к разнообразным последствиям, начиная с кражи личной информации и заканчивая вымогательством денег или потерей ценных данных.

Рассчитывая киберриски и выбирая соответствующие им методы обеспечения информационной безопасности, работа всех сетей передачи данных, компьютерных систем и мобильных устройств становится наиболее надежной и защищенной.

По рассчитанной оценке, киберрисков можно узнать значение потенциального ущерба от киберпреступлений, что позволяет более тщательно подготовится к кибератакам

Используя одновременно все простые надежные и эффективные методы по обеспечению информационной безопасности, уменьшается риск несанкционированного доступа или злонамеренных атак на системы, основанные на оцифровке, интеграции и автоматизации, до минимального значения.

Литература

1. Нейтон Хаус. Полный курс по кибербезопасности: Секреты хакеров. Том 1. 271с.
2. Башлы П. Н., Баранова Е. К., Бабаш А. В. Информационная безопасность: учебно-практическое пособие. – М., Евразийский открытый институт, 2011. – 375с.;
3. Скрипник Д. А. Общие вопросы технической защиты информации. – М., Национальный Открытый Университет «ИНТУИТ», 2016. – 425с.;
4. [Электронный ресурс] Классификация методов защиты информации – Сайт: http://camafon.ru
5. ISO/IEC 27001. Международный стандарт содержит требования в области информационной безопасности для создания, развития и поддержания системы менеджмента информационной безопасности. 20с.
6. ГОСТ ИСО/МЭК ТО 7. Национальный стандарт Российской Федерации. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий. Москва. 20с.
7. BS 7799-2:2005 Спецификация системы управления информационной безопасностью. Англия. 20с.
8. Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.

References

1. Nejton Haus. Polnyj kurs po kiberbezopasnosti: Sekrety hakerov. Tom 1. 271s.
2. Bashly P. N., Baranova E. K., Babash A. V. Informatsionnaja bezopasnost': uchebno-prakticheskoe posobie. – M., Evrazijskij otkrytyj institut, 2011. – 375s.;
3. Skripnik D. A. Obschie voprosy tehnicheskoj zaschity informatsii. – M., Natsional'nyj Otkrytyj Universitet «INTUIT», 2016. – 425s.;
4. [`Elektronnyj resurs] Klassifikatsija metodov zaschity informatsii – Sajt: http://camafon.ru
5. ISO/IEC 27001. Mezhdunarodnyj standart soderzhit trebovanija v oblasti informatsionnoj bezopasnosti dlja sozdanija, razvitija i podderzhanija sistemy menedzhmenta informatsionnoj bezopasnosti. 20s.
6. GOST ISO/M`EK TO 7. Natsional'nyj standart Rossijskoj Federatsii. Metody i sredstva obespechenija bezopasnosti. Chast' 3. Metody menedzhmenta bezopasnosti informatsionnyh tehnologij. Moskva. 20s.
7. BS 7799-2:2005 Spetsifikatsija sistemy upravlenija informatsionnoj bezopasnost'ju. Anglija. 20s.
8. Baranova, E.K. Informatsionnaja bezopasnost' i zaschita informatsii: Uchebnoe posobie / E.K. Baranova, A.V. Babash. - M.: Rior, 2018. - 400 c.