ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004. 094

DOI: 10.21822/2073-6185-2024-51-1-123-131 Обзорная статья / Review article

Проблемы подготовки специалистов в области информационной безопасности

И.И. Лившиц
Национальный исследовательский университет ИТМО,
197101, г.Санкт-Петербург, Кронверкский пр., д. 49, Россия

Резюме. Цель. Проблема подготовки специалистов в области информационной безопасности представляется актуальной с учетом недостатка специалистов, способных оказать противодействие новым угрозам. Объективно наблюдается существенный дефицит квалифицированных специалистов, которых могли бы подготовить технические ВУЗы Российской Федерации в самое ближайшее время. При решении указанной проблемы важно принять во внимание уровень качества выпускаемых специалистов и негативный риск от дистанционного режима обучения. **Метод**. В представленной работе предложен анализ потребностей в квалифицированных специалистах по программе 10.04.01 «Информационная безопасность» и статистический анализ выпускных квалификационных работ магистров факультета ФБИТ Университета ИТМО по итогам работы государственных экзаменационных комиссий 2023 г. **Результат**. Проведен анализ потребностей в квалицированных специалистах в области информационной безопасности на основе доступных данных; показано, что при существующей динамике в ближайшее время не представляется возможным обеспечить необходимое количество квалифицированных специалистов без существенных изменений в ВУЗах. Проведен анализ ВКР магистров, обучающихся по программе 10.04.01 «Информационная безопасность» в аспекте поставленной проблемы: отражены примеры отличного выполнения работ для «индустрии» и риски выполнения типовых «шаблонных» работ. **Вывод**. Представленные результаты могут быть применены для оценки качества подготовки специалистов в области информационной безопасности в технических ВУЗах Российской Федерации в соответствии с известными потребностями, а также с учетом перспективных направлений.

Ключевые слова: программа обучения, компетенции, дистант, требования, информационная безопасность, специальность, меры защиты, риски, остаточные риски

Для цитирования: И.И. Лившиц. Проблемы подготовки специалистов в области информационной безопасности. Вестник Дагестанского государственного технического университета. Технические науки. 2024; 51(1):123-131. DOI:10.21822/2073-6185-2024-51-1-123-131

Problems of training specialists in the field of information security

I.I. Livshits
National Research University ITMO,
49 Kronverksky Ave., St. Petersburg 197101, Russia

Abstract. **Objective**. The problem of training specialists in the field of information security seems relevant given the lack of specialists capable of countering new threats. Objectively, there is a significant shortage of qualified specialists who could be trained by technical universities of the Russian Federation in the very near future. When solving this problem, it is important to take into account the level of quality of the graduates and the negative risk from the distance learning mode. **Method.** The presented work proposes an analysis of the needs for qualified specialists in the program 10.04.01 “Information Security” and a statistical analysis of the final qualifying works of masters of the Faculty of FBIT of ITMO University based on the results of the work of state examination commissions in 2023. **Result.** An analysis of the needs for qualified information security specialists was carried out based on available data; It is shown that given the current dynamics, it is not possible in the near future to provide the required number of qualified specialists without sig-

nificant changes in universities. An analysis of the graduate work of masters studying under the 10.04.01 "Information Security" program was carried out in the aspect of the problem posed: examples of excellent performance of work for the "industry" and the risks of performing standard "template" work were reflected. **Conclusion.** The results can be used to assess the quality of training of specialists in the field of information security in technical universities in Russia.

Keywords: training program, competencies, distance learning, requirements, information security, specialty, protection measures, risks, residual risks

For citation: I.I. Livshits. Problems of training specialists in the field of information security. Herald of Daghestan State Technical University. Technical Sciences. 2024; 51(1):123-131. DOI:10.21822/2073-6185-2024-51-1-123-131

Введение. Современные организации применяют множество самых различных ИТ-систем, соответственно, критичное значение приобретает фактор обеспечения квалифицированным персоналом, способным обеспечить требуемый уровень информационной безопасности (далее – ИБ). Эта проблема известна в системе высшего образования, и в настоящее время экспертами предложено несколько путей решения: например, нанять готового квалифицированного специалиста, проводить собственное обучение или принимать молодых выпускников технических ВУЗов по соответствующим специальностям.

В статье рассматривается вариант подготовки квалифицированных специалистов в области ИБ в Университете ИТМО и методах оценки выпускных квалификационных работ (далее – ВКР). Рассмотренная проблема доступности нужного количества квалифицированного персонала подтверждается на уровне регуляторов, в частности в приказе Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России) от 20.04.2023 № 69 «О внесении изменений в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом ФСТЭК России от 21 декабря 2017 г. № 235». Полученные результаты могут быть применены для оценки качества подготовки специалистов в области ИБ в технических ВУЗах РФ в соответствии с текущими потребностями, а также с учетом перспективных направлений.

Постановка задачи. Известна позиция экспертов (например, Positive Technologies), что «недостаток квалифицированных кадров может приводить к пониженной эффективности систем». Аналогичные суждения приведены в докладе Центрального Банка России на «Инфофоруме-Сочи 2023» – объем средств, похищенных кибермошенниками в Российской Федерации с начала 2023 г., достиг 4,5 млрд. руб., по сравнению со средними значениями 2022 г. объем похищенных средств вырос почти на 30%.

В настоящее время работодатели реагируют вполне адекватно, в частности, существенно меняются приоритеты служб, но остаточный риск все же достаточно велик – доля компаний, которые объективно подтверждают нехватку кадров, выросла в 2023 г. до значения 50%. Соответственно, компании увеличивают расходы на собственное корпоративное обучение, например, крупнейшие компании, как правило, имеют собственные учебные центры. По данным Group-IB количество запросов на обучение специалистов выросло на 30% год, наибольший спрос наблюдается на обучение специалистов-практиков и технических специалистов. Оценки компании Positive Technologies более значительные – зафиксирован рост более чем на 70%.

Методы исследования. Рассмотрим более внимательно третий вариант решения проблемы – подготовку квалифицированных специалистов в технических ВУЗах РФ. Известны публикации по данной тематике [1- 4]. В докладах XXVIII научно-практической конференции «Комплексная защита информации» (г. Гомель, Республика Беларусь), проблеме обеспечения качества образования и выпуска специалистов в области ИБ уделялось особое внимание. В докладе директора ЦПК ИБ РТУ МИРЭА представлено описание про-

блемы подготовки кадров в области ИБ и значительное количество актуальных и объективных аналитических данных (рис. 1).

Рис. 1. Базовый показатель потребности в специалистах по ИБ
Fig. 1. Basic indicator of the need for information security specialists

На представленном рис. 1 показана слабая (в пределах 16% – 11%) линейная динамика показателя на интервале 2018 – 2023 гг., не в полной мере отражающая новые риски потребности в значительном увеличении количества специалистов по ИБ. Данные по контрольным цифрам приема (далее – КЦП) по направлению ИБ представлены на рис. 2. Важно, что совокупная возможность технических ВУЗов в Российской Федерации (бакалавры, магистры и специалисты) не превышает 9 тыс. человек по состоянию на 2022 г.

Подготовка по УГСНП 10.00.00 «Информационная безопасность»

Контрольные цифры приема граждан на 2017 - 2022 г.

Уровни образования	2017	2018	2019	2020	2021	1 этап 2022
Бакалавриат	2287	2379	2324	2890	3473	3556
Магистратура	953	999	566	608	615	712
Специалитет	3158	3264	3127	3743	4344	4381
Итого	**6398**	**6642**	**6017**	**7241**	**8432**	**8649**

Рис. 2. Контрольные цифры приема по специальностям ИБ
Fig. 2. Target numbers for admission to information security specialties

В рассматриваемом докладе приводится также экспертная оценка потребности в специалистах ИБ в 20 тыс. человек, что превышает представленные выше совокупные возможности системы ВУЗов в РФ минимум вдвое. Более того, дается экспертная оценка собственных возможностей ВУЗов по направлению подготовки кадров высшей квалификации – при ежегодной потребности в 670 чел. объемы подготовки составляют всего 16 чел., что составляет только 2,4%. В докладе ФСТЭК России приведены примеры разработанных видео-лекций для специалистов в области ИБ, которые размещены на собственных ресурсах БДУ ФСТЭК России и результаты анализа уровня квалификации специалистов по защите информации (рис. 3).

Рис. 3. Результаты анализа уровня квалификации специалистов по защите информации
Fig. 3. Results of analysis of the level of qualifications of information security specialists

Этот пример хорошо иллюстрирует особенности рассматриваемой проблемы – доля специалистов, не имеющих никакого образования в области ИБ, составляет в организациях, оказывающих услуги по защите информации всего 4,5%.

В области оборонно-промышленного комплекса доля специалистов, не имеющих образования в области ИБ, составляет 47,9%, что частично может быть уравновешено специалистами, прошедшими переподготовку в области ИБ (37%) и/или имеющих базовое образование в области ИБ (15%).

В сегменте органов исполнительной власти наблюдается, к сожалению минимальная доля специалистов, прошедших переподготовку в области ИБ (около 23%) и максимальная доля специалистов, не имеющих образования в области ИБ (около 62%).

Обсуждение результатов. Рассмотрим примеры исключительных и недостаточно успешных примеров ВКР по специальности 10.04.01 «Информационная безопасность» по итогам работы ГЭК факультета ФБИТ в Университете ИТМО за 2023 г.

Важно принять во внимание, что на полученные результаты негативное влияние оказали последствия дистанционного режима обучения, поскольку были существенно нарушены привычные коммуникации обучающихся и преподавателей ВУЗов. Этот тезис подтверждается достаточным количеством экспертных мнений, например, в аналитической статье [17] по итогам оценки результатов ЕГЭ в 2023 г. отмечено, цитата: «Эксперт уверена: это происходит в том числе потому, что московским школам удалось избежать падения уровня образования во время пандемии». Некоторые данные по дистанционному режиму обучения представлены в работах автора [5 – 7] и других исследователей [8 – 11].

Сначала предлагается рассмотреть некоторые не слишком успешные примеры ВКР, которые были своевременно выявлены при многоэтапной экспертизе на факультете ФБИТ и приведены в соответствие. Персональные данные все примеров скрыты по соображениям конфиденциальности.

Пример 1. В представленной на согласование ВКР по теме защиты станка с ЧПУ были две таблицы (табл.1 и табл.2), в которых были приведены типы активов, распределение ценностей этих активов по известной триаде «КДЦ» (конфиденциальность, доступность и целостность) и оценки степени уязвимостей на основании БДУ ФСТЭК [18], соответственно.

Таблица 1. Шкала ценности активов (фрагмент)
Table 1. Asset value scale (fragment)

Идентификатор актива/ Asset ID	**Активы организации Organizational assets**	**Конфиденциальность Confidentiality (К)**	**Целостность Integrity (Ц)**	**Доступность Availability (Д)**	**Ценность актива Asset value**
A	Физические машины/ Physical machines	–	3	4	4
B	Процессы/ Processes	2	4	4	4
C	Интеллектуальная собственность/ Intellectual property	2	2	1	2
D	Информация/ Information	2	3	2	3
E	Персонал / Staff	–	1	1	1
F	Место функционирования организации/ Place of operation of the organization	–	1	1	1
G	Сеть/ Net	–	3	4	4
H	Аппаратно-программный комплекс/ Hardware and software complex	–	3	4	4

Таблица 2. Степень уязвимости актива (фрагмент)
Table 2. Degree of asset vulnerability (fragment)

УБИ	Идентификатор актива Asset ID							
	A	B	C	D	E	F	G	H
6	–	–	–	–	–	–	1	2
7	–	–	–	–	–	–	2	2
8	–	–	–	1	–	–	1	1
30	–	–	–	1	–	–	1	2
31	–	–	–	1	–	–	1	1
34	–	–	–	–	–	–	3	–
63	–	–	–	–	–	–	–	3
69	–	–	–	–	–	–	1	–
107	3	2	**2**	–	**1**	1	–	–
112	3	2	**2**	–	**1**	–	–	–
122	–	2	**–**	–	**2**	–	–	–
183	3	2	**2**	–	**1**	–	–	–
204	3	2	**–**	–	**2**	–	–	–

При анализе данного примера обратим внимание на 3 обстоятельства:

1) Выбран пример организации, в активе которой есть станки с ЧПУ, соответственно, в состав активов включены и материальные активы («машины», «сеть», «программно-аппаратный комплекс»), так и нематериальные активы («интеллектуальная собственность» (тип С) и «персонал» (тип Е), соответственно);

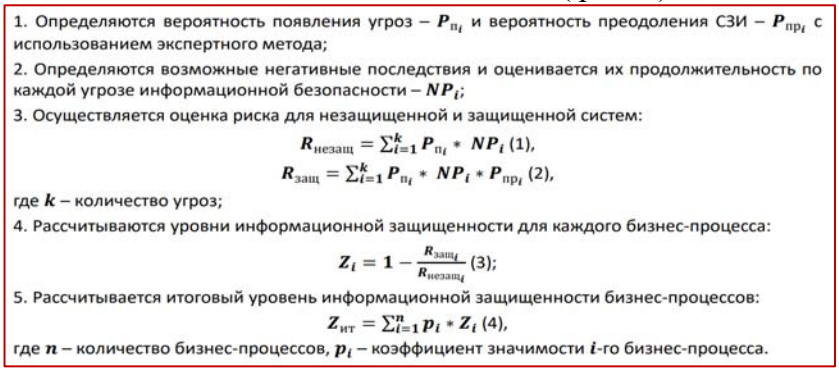
2) Применена известная методическая база угроз БДУ ФСТЭК, конкретно для примеров активов тип С и тип Е выбраны:

- УБИ 107 – Угроза отключения контрольных датчиков;
- УБИ 112 – Угроза передачи запрещённых команд на оборудование с ЧПУ;
- УБИ 122 – Угроза повышения привилегий;
- УБИ 183 – Угроза перехвата управления АСУТП;
- УБИ 204 – Угроза несанкционированного изменения вредоносной программой значений параметров ПЛК.

3) Выполнена унифицированная оценка степени уязвимости активов по единой базе угроз БДУ ФСТЭК, в том числе для нематериальных активов (С и Е).

При более вдумчивом рассмотрении представленного проекта ВКР было обращено внимание, что для активов С и Е признаны актуальными УБИ 107, УБИ 112 и УБИ 183, а для актива Е (персонал) еще и УБИ 122 и УБИ 204. Сложно представить логику обучающего, которые полагает актуальной угрозу отключения контрольных датчиков или перехвата управления для персонала (человека, а не «железа»), обслуживающего станок с ЧПУ и уж совсем невозможно представить угрозу изменения вредоносной программой такого объекта, как «человек». Вполне вероятно, что подобная ситуация явилась прямым следствием дистанционного режима обучения, бездумного применения методических документов ФСТЭК России и непонимания «физики» процессов обеспечения безопасности для различных типов активов.

Пример 2. В одной ВКР, представленной на согласование, был предложен вариант расчета риска для незащищенной и защищенных систем (рис. 4)


1. Определяются вероятность появления угроз – $P_{п_i}$ и вероятность преодоления СЗИ – $P_{пр_i}$ с использованием экспертного метода;
2. Определяются возможные негативные последствия и оценивается их продолжительность по каждой угрозе информационной безопасности – NP_i;
3. Осуществляется оценка риска для незащищенной и защищенной систем:

$$R_{незащ} = \sum_{i=1}^{k} P_{п_i} * NP_i \ (1),$$

$$R_{защ} = \sum_{i=1}^{k} P_{п_i} * NP_i * P_{пр_i} \ (2),$$

где k – количество угроз;
4. Рассчитываются уровни информационной защищенности для каждого бизнес-процесса:

$$Z_i = 1 - \frac{R_{защ_i}}{R_{незащ_i}} \ (3);$$

5. Рассчитывается итоговый уровень информационной защищенности бизнес-процессов:

$$Z_{ит} = \sum_{i=1}^{n} p_i * Z_i \ (4),$$

где n – количество бизнес-процессов, p_i – коэффициент значимости i-го бизнес-процесса.

Рис. 4. Пример расчета риска для незащищенной и защищенных систем
Fig. 4. Example of risk calculation for unprotected and protected systems

При анализе данной работы вызывает удивление размерность рассчитываемого риска. В соответствии с приведенными выше формулами, риск должен бы измеряться во времени (вероятность – величина безразмерная, а негативные последствия предложено измерять по времени продолжительности каждой угрозы). Более того, предложенные в варианте ВКР формулы дают весьма спорные результаты. Далее в табл. 3 показаны примеры расчета по предложенным формулам для нескольких «граничных» значений параметров.

Таблица 3. Пример расчета риска для незащищенной и защищенных систем
Table 3. Example of risk calculation for unprotected and protected systems

$P_{п1}$	$P_{п2}$	$P_{пр1}$	$P_{пр2}$	$H_{п1}$	$H_{п2}$	$P_{незащ}$	$P_{защ}$	Риск	Сценарий
0,6	0,4	0,1	0,2	10	12	10,8	1,56	0,86	Хорошие СЗИ и средние угрозы (неравные) /Good SZ and average threats (unequal)
0,5	0,5	0,5	0,5	10	12	11	5,5	0,50	Средние СЗИ и средние угрозы (равные)/ Average SZI and average threats (equal)
0,1	0,1	0,1	0,1	10	12	2,2	0,22	0,90	Хорошие СЗИ и низкие угрозы/ Good security information and low threats
0,1	0,1	0,9	0,9	10	12	2,2	1,98	0,10	Плохие СЗИ и низкие угрозы/ Poor security information and low threats
0,9	0,9	0,1	0,1	10	12	19,8	1,98	0,90	Хорошие СЗИ и высокие угрозы/ Good information security and high threats
0,9	0,9	0,9	0,9	10	12	19,8	17,82	0,10	Плохие СЗИ и высокие угрозы/ Poor information security and high threats

На графике (рис. 5) для нескольких простых сценариев объективно следует, что величина риска существенным образом должна бы зависеть только от «качества» работы применяемых мер защиты (варианты 4 и 6, где вероятность преодоления СЗИ принята равной 90%). В иных случаях (варианты 3 и 5), даже при «разбросе» вероятности реализации УБИ от 10% до 90% значение риска будет практически максимальным – 90% при заданных граничных условиях. Первые два варианта дают оценочное суждение при среднем уровне вероятности УБИ и, соответственно, средней и минимальной вероятности преодоления СЗИ.

Рис. 5. Пример оценки рисков при реализации УБИ
Fig. 5. Example of risk assessment when implementing UBI

Пример 3. В проект ВКР была предложена следующая формулировка, цитата: «Объективно, дать единое, точное и универсальное определение понятию «информация» в течение настоящего времени и ближайшего будущего в период, доступный для мысленного анализа, возможным не представляется.

Соответственно, выполнение каких-либо операций, направленных на взаимодействие с информацией как с отдельно взятой во времени и пространстве сущностью, то есть требующих выполнения работ не только с ее содержанием, но также и независимо от него, предполагает раскрытие данного понятия непосредственно в рамках исследуемой области человеческой деятельности». При обсуждении указанного проекта ВКР выяснилось, что помимо вольного изложения ничем не обоснованного предположения и иных весьма «оригинальных» фрагментов текста, практически отсутствуют минимальные знания в области нор-

мативно-методической базы, актуальных стандартов, содержащих необходимые термины и определения в области ИБ, нет основательных знаний в области оценки энтропийных процессов и требуемого навыка выполнения научных исследований.

Далее будут рассмотрены несколько наиболее выдающихся ВКР, которые заслуженно получили высший балл и были отмечены особо по итогам работы ГЭК факультета ФБИТ Университета ИТМО. На рис. 6 представлен пример сопоставления результатов расчета уровня полноты безопасности (далее – УПБ) при обеспечении функциональной безопасности конкретного семейства отечественных ПЛК. Особая ценность данного расчета заключается в простой и объективной форме представления реально достижимого УПБ для разных архитектур ПЛК в составе объектов КИИ.

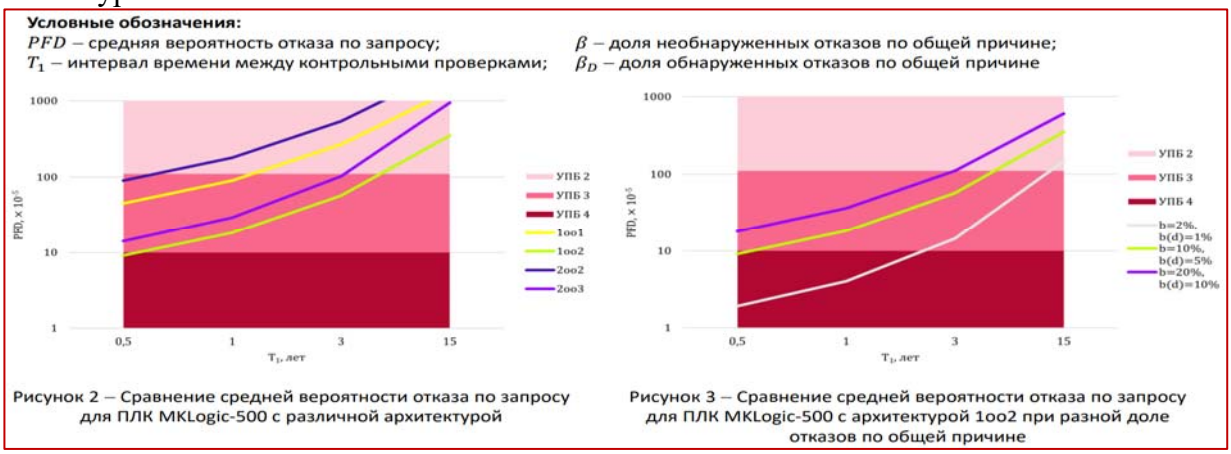


Рисунок 2 – Сравнение средней вероятности отказа по запросу для ПЛК MKLogic-500 с различной архитектурой

Рисунок 3 – Сравнение средней вероятности отказа по запросу для ПЛК MKLogic-500 с архитектурой 1oo2 при разной доле отказов по общей причине

Рис. 6. Пример расчета уровня полноты безопасности
Fig. 6. Example of safety integrity level calculation

На рис. 7 представлен удачный пример эффективного применения математического аппарата для оценки различных методик контроля уровня защищенности.

Таблица 5 – Оценка по Парето различных вариантов для оценки защищенности объектов КИИ

Вектор оценок	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
$y^{(1)}$	2	2	1	1	2	2	3	2
$y^{(2)}$	2	3	2	1	3	4	3	3
$y^{(3)}$	**3**	**4**	**2**	**2**	**4**	**4**	**5**	**4**

Рис. 7. Пример математического обоснования методик контроля уровня защищенности
Fig. 7. An example of mathematical substantiation of methods for monitoring the level of security

Выполнено математическое обоснование методики контроля уровня защищенности информации:

- $y^{(1)}$ – оценка (анализ) защищенности (требования: проекты методики ФСТЭК России);
- $y^{(2)}$ – оценка состояния защиты информации (обеспечения безопасности) в органе (организации) (требования: проект методики ФСТЭК России);
- $y^{(3)}$ – методика контроля уровня защищенности информации объектов КИИ (требования: документы ФСТЭК России, дополнительные международные стандарты и методики).

Полученные результаты объективно позволяют оценивать текущие и перспективные методики контроля уровня защищенности информации. Можно отметить, что подобные расчеты известны и в международных публикациях, но их число невелико [12 – 16].

На рис. 8 представлен хороший пример цифровой интерпретации численных показателей оценки уровня ИБ для различных мер защиты в соответствии с требованиями ГОСТ Р ИСО/МЭК серии 27001. Представленный пример позволяет оперативно отображать в собственном программном продукте результаты вдумчивого анализа нескольких вариантов реализации мер ИБ (например, по требованиям ГОСТ Р ИСО/МЭК серии 27001 или Приказа

ФСТЭК России №239). В ВКР отмечено, как подобная практика была применена на реальных проектах по оценке степени соответствия «боевых» систем.

Рис. 8. Пример расчета показателей оценки уровня ИБ

Fig. 8. An example of calculating indicators for assessing the level of information security

Вывод. Проблема увеличения качества квалифицированных специалистов по направлению ИБ представляется особенно актуальной с учетом известных инцидентов компрометации ИТ-инфраструктуры крупных компаний. По оценкам экспертов в настоящее время наблюдается дефицит доступных квалифицированных специалистов, и критическая ситуация с возможностью технических ВУЗов Российской Федерации увеличить выпуск специалистов. Проведен анализ ВКР магистров, обучающихся в Университете ИТМО по программе 10.04.01 «Информационная безопасность» в аспекте поставленной проблемы. Представленные результаты могут быть применены для оценки качества подготовки квалифицированных специалистов в области ИБ в ВУЗах Российской Федерации.

Библиографический список:

1. Курило А.П. Реализация в МЛГУ новых стандартов обучения по специальности «Информационной безопасность». В книге: Комплексная защита информации. Материалы XXVI научно-практической конференции. Ответственный за выпуск Касанин С. Н. - доцент, канд. техн. наук. 2021. С. 162-164.
2. Давудов Д.А., Ханова Т.С. Актуальные вопросы обучения студентов ВУЗов основам информационной безопасности в области защиты прав интеллектуальной собственности // Вестник педагогических наук. 2020. № 3. С. 104-111.
3. Влацкая И.В., Джукашев К.Р. Эффективное обучение программированию специалистов информационной безопасности в условиях импортозамещения // Научно-технический вестник Поволжья. 2023. № 3. С. 184-188.
4. Малюк А.А., Малюк З.П. Актуальные вопросы создания систем массового обучения культуре информационной безопасности//Безопасность информационных технологий. 2021. Т. 28. № 4. С. 6-21.
5. Лившиц И.И. Управление качеством в дистанционном режиме обучения на примере практики в Университете ИТМО // Менеджмент качества. 2022. № 1. С. 68-77.
6. Лившиц И.И. Результаты применения воронки рисков в полном дистанционном режиме обучения // Энергобезопасность и энергосбережение. 2021. № 2. С. 46-50.
7. Лившиц И.И. Дистанционный формат обучения: риски и возможности // Стандарты и качество. 2020. №10. С. 102-107.
8. Гавриленко А.В. Дистанционное обучение и информационная безопасность // Вестник РГГУ. Серия: Информатика. Информационная безопасность. Математика. 2021. № 1. С. 51-65.
9. Базаргулов Э.Э., Докторов О.П. Обеспечение информационной безопасности при дистанционном обучении // В сборнике: Наука и техника: новые вызовы современности. Сборник статей IV Международной научно-практической конференции. г. Москва, 2022. С. 9-12.
10. Стеньшина Т.Д. Разработка модели информационной безопасности для дистанционного обучения в ВУЗе // Студенческий вестник. 2022. № 23-9 (215). С. 46-50.
11. Бурховецкая О.В., Кузина Н.Н. Обеспечение информационной безопасности при переходе на дистанционное обучение // Вопросы педагогики. 2020. № 6-2. С. 55-57.

12. Kweon E., Lee H., Chai S., Yoo K. The utility of Information security training and education on cybersecurity incidents: An empirical evidence. Information Systems Frontiers. 2021. Т. 23. № 2. С. 361-373.
13. Yang G., Dineen S., Lin Z., Liu X. Few-sample named entity recognition for security vulnerability reports by fine-tuning pre-trained language model. Communications in Computer and Information Science. 2021. Т. 1482. С. 55-78.
14. Weatherford D.R., Roberson D., Erickson W.B. When experience does not promote expertise: Security professionals fail to detect low prevalence fake IDS. Cognitive Research. 2021. Т. 6. № 1. С. 1-27.
15. Liu P., Xu X., Wang W. Threads, attacks and defenses to federate learning: Issues, taxonomy and perspectives. Cybersecurity. 2022. Т. 5. № 1. С. 1-19.
16. Qammar A., Ding J., Ning H. Federated learning attack surface: Taxonomy, cyber defenses, challenges and future directions. Artificial Intelligence Review. 2022. Т. 55. № 5. С. 3569-3606.
17. https://www.kommersant.ru/doc/6111520?from=glavnoe_3
18. https://bdu.fstec.ru/threat

References

1. Kurilo A.P. Implementation of new training standards in the specialty “Information Security” at MLSU. In the book: Comprehensive information protection. Materials of the XXVI scientific and practical conference. Responsible for the issue is Kasanin S.N. - Associate Professor, Candidate of Sciences. tech. Sci. 2021; 162-164. (In Russ)
2. Davudov D.A., Khanova T.S. Topical issues of teaching university students the basics of information security in the field of protection of intellectual property rights. *Bulletin of Pedagogical Sciences*. 2020; 3:104-111. (In Russ)
3. Vlatskaya I.V., Dzhukashev K.R. Effective programming training for information security specialists in the conditions of import substitution. *Scientific and Technical Bulletin of the Volga Region*. 2023; 3:184-188. (In Russ)
4. Malyuk A.A., Malyuk Z.P. Topical issues of creating systems for mass training in the culture of information security. *Security of information technologies*. 2021; 28(4): 6-21(In Russ)
5. Livshits I.I. Quality management in distance learning based on the example of practice at ITMO University. *Quality Management*. 2022; 1: 68-77. (In Russ)
6. Livshits I.I. Results of using the risk funnel in full distance learning mode. *Energy safety and energy saving*. 2021; 2: 46-50. (In Russ)
7. Livshits I.I. Distance learning format: risks and opportunities. *Standards and quality*. 2020;10: 102-107. (In Russ)
8. Gavrilenko A.V. Distance learning and information security. *Bulletin of the Russian State University for the Humanities. Series: Computer Science. Information Security. Mathematic*s. 2021;1:51-65. (In Russ)
9. Bazargulov E.E., Doktorov O.P. Ensuring information security during distance learning. *In the collection: Science and technology: new challenges of modern time*. Collection of articles of the IV International Scientific and Practical Conference. Moscow, 2022: 9-12. (In Russ)
10. Stenshina T.D. Development of an information security model for distance learning at a university. *Student Bulletin.* 2022; 23-9 (215): 46-50. (In Russ)
11. Burkhovetskaya O.V., Kuzina N.N. Ensuring information security during the transition to distance learning. *Questions of pedagogy*. 2020; 6-2.: 55-57.
12. Kweon E., Lee H., Chai S., Yoo K. The utility of Information security training and education on cybersecurity incidents: An empirical evidence. *Information Systems Frontiers*. 2021; 23(2):361-373.
13. Yang G., Dineen S., Lin Z., Liu X. Few-sample named entity recognition for security vulnerability reports by fine-tuning pre-trained language model. *Communications in Computer and Information Science*. 2021; 1482:55-78.
14. Weatherford D.R., Roberson D., Erickson W.B. When experience does not promote expertise: Security professionals fail to detect low prevalence fake IDS. *Cognitive Research*. 2021; 6(1):1-27.
15. Liu P., Xu X., Wang W. Threads, attacks and defenses to federate learning: Issues, taxonomy and perspectives.*Cybersecurity*. 2022; 5(1):1-19.
16. Qammar A., Ding J., Ning H. Federated learning attack surface: Taxonomy, cyber defenses, challenges and future directions. *Artificial Intelligence Review*. 2022.;55(5):3569-3606.
17. https://www.kommersant.ru/doc/6111520?from=glavnoe_3
18. https://bdu.fstec.ru/threat

Сведения об авторе:
Лившиц Илья Иосифович, доктор технических наук, профессор практики, Livshitz.i@yandex.ru
Information about author:
Ilya I. Livshits, Dr. Sci.(Eng.), Prof. of Practice; Livshitz.i@yandex.ru

Конфликт интересов/Conflict of interest.
Автор заявляет об отсутствии конфликта интересов/The author declare no conflict of interest.
Поступила в редакцию/ Received 30.09.2023.
Одобрена после рецензирования/ Reviced 19.12.2023.
Принята в печать/ Accepted for publication 19.12.2023.