УДК 004.056.5, 378 DOI: 10.37468/2307-1400-2020-2-43-49

ФЕДОРОВ ДМИТРИЙ ЮРЬЕВИЧ,
ВЕРЗИЛОВА АРИНА СЕРГЕЕВНА,
ХОРОШЕНКО ВИКТОРИЯ СЕРГЕЕВНА,
БУЙНЕВИЧ МИХАИЛ ВИКТОРОВИЧ

ЭТАПНЫЕ КОМПОНЕНТЫ ДЕЛОВЫХ ИГР ПРИ ОБУЧЕНИИ СТУДЕНТОВ ПОСТРОЕНИЮ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

АННОТАЦИЯ

В статье рассматриваются вопросы, связанные с необходимыми этапными компонентами проектирования деловых игр для обучения студентов построению комплексной системы защиты информации на предприятии: особенности анализа исходных данных экономического субъекта, необходимость проведения оценки рисков в условиях динамики внешнего мира, обеспечение вариативности построения стратегии защиты, формирование объективной оценки эффективности построенной участниками системы защиты.

Ключевые слова: деловые игры; комплексная система защиты информации; оценка рисков; подготовка кадров.

FEDOROV D.Y.,
VERZILOVA A. S.,
KHOROSHENKO V. S.,
BUINEVICH M. V.

STAGE COMPONENTS OF BUSINESS GAMES WHEN TRAINING STUDENTS IN BUILDING AN INTEGRATED INFORMATION PROTECTION SYSTEM

ABSTRACT

The article discusses issues related to the necessary stage components of designing business games for teaching students to build an integrated information security system at an enterprise: features of the analysis of the initial data of an economic entity, the need to conduct a risk assessment in the context of the dynamics of the external world, ensuring the variability of building a protection strategy, forming an objective assessment the effectiveness of the protection system built by the participants.

Keywords: business games; an integrated information security system; risk assessment; training.

Автоматизация всех процессов современного бизнеса и расширение области применения цифровых сервисов и технологий создают потребность в обеспечении защиты информационных ресурсов отдельных пользователей, организаций и государства в целом. Широкий перечень требований, предъявляемых современным рынком труда к специалистам по информационной безопасности (ИБ), обусловлен ценностью обрабатываемой в компании информации, сложностью задач по обеспечению комплексной защиты, а также растущим количеством специалистов по данному направлению [1].

В целях отбора квалифицированных кадров работодатели оценивают не уровень образования и количество научных публикаций потенциального работника, но в большей степени его практический опыт в области ИБ. В этих условиях востребованными на рынке труда становятся специалисты, получившие в вузе профессиональную практико-ориентированную подготовку [2].

В большинстве учебных заведений, реализующих подготовку кадров по ИБ, для закрепления полученных навыков используют семинарские занятия и лабораторные работы по установке, настройке и эксплуатации средств (СрЗИ) и систем защиты информации (СЗИ). Такой подход позволяет студентам ознакомиться с конкретным СрЗИ и его характеристиками в условиях, приближенных к реальным [3]. На рабочем месте будущему специалисту потребуется применять методы и СрЗИ в условиях ограниченного времени и бюджета. Для имитации условий реальных производственных процессов в качестве образовательного инструмента предлагается использовать деловые игры.

Особенность данного инструмента состоит в моделировании среды, в которой отрабаты-

вается способность участника анализировать специфические кейсы и осуществлять поиск решений профессиональных задач в условиях конфликтных ситуаций [4]. Получение и закрепление практических навыков защиты объекта информатизации также подразумевает наличие непосредственно самого объекта информатизации – организации [5].

При создании и проведении деловой игры для обучения специалистов по ИБ необходимо обеспечить формирование профессиональных компетенций и получение практических навыков по построению комплексной системы защиты информации (КСЗИ). Таким образом, разработка деловых игр в области ИБ должна включать следующие этапные компоненты:

1) анализ исходных данных (инфраструктуры организации, описание рынка услуг, особенности деятельности компании, материально-техническое обеспечение и др.), определение информационных ресурсов, подлежащих защите, угроз безопасности информации и возможных путей их реализации для проектирования подсистем и средств обеспечения ИБ;

2) идентификация, анализ и оценка рисков ИБ на основе данных о компании;

3) построение стратегии защиты и ее реализация при помощи конкретных актуальных средств и методов защиты с учетом технико-экономического обоснования соответствующих проектных решений;

4) управление инцидентами, их расследование и анализ для последующей модернизации существующей системы защиты.

Приведенные элементы представляют собой последовательные циклично осуществляемые шаги по построению КСЗИ. Деловая игра в области ИБ должна имитировать перечисленные этапы.

Остановимся подробнее на каждом из этапов.

1) Анализ исходных данных. Организации обрабатывают уникальные данные, что подразумевает специфичные требования к построению КСЗИ на предприятии и ее реализации.

Проектируемая деловая игра должна имитировать процесс аналитического описания специалистом экономического субъекта (организации), а также определения объектов защиты и выявление уязвимостей. Для построения системы защиты в качестве исходных данных сотрудником отдела безопасности изучается показатель исходной защищенности конкретного субъекта безопасности, который на практике вычисляется организациями индивидуально.

Например, задаются элементы корпоративной информационной системы (ИС), которые в упрощённом виде представлены на рисунке 1.

1. На АРМах установлена ОС Windows 7.
2. На АРМах созданы ученые записи для каждого пользователя, который за ним работает, а также учетная запись администратора.
3. На компьютере бухгалтера установлена программа 1С Бухгалтерия. Предприятие.
4. На АРМах оформителей установлены программы: Adobe Photoshop и Adobe Illustrator. Работники могут также устанавливать необходимое ПО самостоятельно.
5. На всех ПК установлен пакет Microsoft Office.
6. На АРМах службы работы с клиентами установлен SQL Server Managment. Один из АРМов используеся в качестве ИСПДн.
7. В кабинете директора установлен Wi-Fi роутер.
8. Работа на дому и на собственных машинах запрещена.
9. В рабочие часы помещения отрыты. Ключи есть у начальников каждого отдела. В обед сотрудники могут остаться в офисе, или могут пойти пообедать.
10. Информация, обрабатываемая в каждом отделе, хрнится на АРМах этого отдела.
11. Персонал подбирается кадровым агенством, которое анализирует прошлые места работы, опыт, квалификацию.

Рисунок 1 – Элементы корпоративной ИС

Участники игры оценивают показатель исходной защищенности на основе предоставленных данных и могут сделать выводы о низком уровне защищенности организации. Специалисты по защите информации должны обратить внимание на следующие аспекты:

– отсутствие данных о наличии сертификата используемых информационных продуктов;
– наличие открытого доступа к глобальной сети;
– наличие свободного доступа к помещению, в котором обрабатывается информация закрытого доступа;
– наличие системы разграничения доступа;
– отсутствие средств резервного копирования и т.д.

Определение границ системы управления ИБ и уточнение ее целей является начальным этапом разработки концепции защиты информации. Организационная структура компании и ее политика в отношении защиты данных задают ограничения полномочий специалистов и особенности технологических процессов по защите информации. Для построения эффективной системы защиты информации требуется определить цель защиты и ее направления, то есть дифференцировать по значимости отдельные объекты, требующие защиты.

Например, участники игры получают описание деятельности организации и ее активов, представленные на рисунке 2.

Деятельность компании	Обрабатываемая информация
Компания занимается печатью художественных произведений, текст которых получает от собственников. Текст произведений является интеллектуальной собственностью авторов.	Компания работает с интеллектуальной собственностью заказчиков (тексты произведений), интеллектуальной собственностью компании (обложки, разработанные оформителями и пр.), обрабатываются персональные данные клиентов, а также кадровая и служебная информация.

Рисунок 2 – Описание деятельности компании

На основании полученных данных участники формируют направления защиты, ранжируя по степени ценности для компании категории защищаемой информации:

– интеллектуальная собственность компании (как информационный ресурс, обеспечивающий основную прибыль компании);
– интеллектуальная собственность заказчиков (как ресурс, влияющий на репутационные активы компании);
– персональные данные клиентов (как защищаемая информация на государственном уровне и ресурс, влияющий на репутационные активы компании);
– кадровая и служебная информация (как защищаемая информация на государственном уровне и ресурс, влияющий на прибыль компании).

Стоимость системы защиты не должна превышать стоимости самой защищаемой информации, что обуславливает необходимость анализа финансовых потоков рассматриваемой организации и оценки ценности информации.

2) Оценка рисков. Деловая игра должна предусматривать процесс оценки рисков, масштабируемый в условиях проведения игры в формате учебного занятия. В рамках прохождения программы обучения по ИБ происходит знакомство с различными методиками оценки рисков. Внешняя среда функционирования современных компаний задает высокую динамику изменения приоритетов и направлений, в результате чего оценка рисков превращается в процесс. В связи с этим, при проектировании деловой игры по ИБ необходимо обеспечить постоянный мониторинг оценки рисков и угроз, например, в виде случайных изменений внешних условий для приближения игровой модели к реальным условиям производственного процесса.

Например, для каждого цикла деловой игры (игрового года) вводятся изменения игрового мира, влияющие на вероятности реализации потенциальных угроз, представленные в таблице 1.

Таблица 1

Варианты изменения внешней среды

№	*Изменение внешней среды*	*Влияние на состояние защищённости компании*
1	Переход на дистанционный формат работы	повышается вероятность непреднамеренных действий пользователей и угроз, реализуемых с использованием каналов связи (сетевых угроз)
		уменьшается вероятность реализации угроз неатропогенного характера, угроз, связанных с физическим доступом и техническими каналами утечки
2	Банкротство кадрового агентства	увеличивает риски некачественного подбора персонала, в связи с чем увеличивается вероятность реализации угроз преднамеренных действий пользователей, непреднамеренных действий пользователей и угроз хищения и уничтожения путем физического доступа
3	Ликвидация охраны бизнес-центра/ЧОП	повышается вероятность реализации угроз утечки по техническим каналам, угроз хищения и уничтожения путем физического доступа
4	Сотрудничество с государственными органами	устанавливает необходимость наличия сертифицированных СрЗИ и системы менеджмента ИБ

Кроме того, специалисты по ИБ должны обладать способностью определять уязвимости существующей системы защиты и потенциально возможные угрозы с определением степени их актуальности для конкретного экономического субъекта в заданных условиях.

На основе анализа полученной информации участники могут определить наиболее вероятные угрозы с учетом показателя исходной защищенности:

- угрозы непреднамеренных действий пользователей;
- угрозы, связанные с использованием программных решений;
- угрозы преднамеренных действий внутренних нарушителей;
- угрозы несанкционированного доступа по каналам связи;
- угрозы от утечки по техническим каналам.

Таким образом, в рамках игры необходимо предусмотреть следующие аспекты:

- отображение разнообразных причин реализации угроз;
- моделирование конкретных ситуаций реализации угроз;
- наличие вариативности возможных исходов реализации угроз;
- имитация условий внешней среды.

3) Построение стратегии защиты. Основной этап деловой игры имитирует построение стратегии защиты критической информации. В целях приближения моделируемого игрового пространства к реальным условиям современного бизнеса требуется введение ограничений на необходимые ресурсы, в том числе финансовые, временные и пр.

Для обеспечения финансовых ограничений необходимо ввести систему игровой валюты, в которой будет измеряться выделенный на ИБ бюджет, а также стоимость предлагаемых СрЗИ. Стоимость СрЗИ может представлять собой реальные цены на рынке услуг и продуктов, перенесенные в пропорции игровой валюты. Соотношение бюджета ИБ со стоимостью предлагаемых решений должно обеспечивать возможность построения лучшей стратегии защиты при реализации принципов разумности, достаточности и необходимости.

Построение системы защиты производится от общих концепций к частным решениям. Для построения стратегии защиты при проектировании деловой игры требуется сформировать перечень предлагаемых участникам средств и методов защиты, реализующих защиту информации на организационно-правовом, программно-аппаратном, инженерно-техническом и криптографическом уровнях. Для обеспечения вариативности сценариев игры необходимо предусмотреть возможность построения эффективной системы защиты разными наборами предлагаемых средств.

В приведенном примере участники могут

выбрать СрЗИ, которые необходимы для предотвращения актуальных угроз с учетом анализа исходных данных и особенностей (или изменений) внешней среды:

- антивирусное ПО;
- построение системы менеджмента ИБ (разработка политики безопасности, инструктаж работников и пр.);
- настройка резервного копирования;
- DLP-системы и настройка разграничения доступа;
- установка видеонаблюдения и приобретение средств обнаружения закладных устройств и т.д.

Для реализации построенной участниками стратегии защиты необходимо обеспечить имитацию реального рынка продуктов и услуг, предоставляемых в сфере ИБ. Данный аспект требует соблюдения требований к предлагаемым решениям:

- актуальность (широкое использование в бизнесе);
- осведомленность (предварительное знакомство в период обучения);
- обеспечение защиты от актуальных для моделируемой организации угроз;
- наличие информации о принципах действия в открытом доступе.

Для обеспечения широкого выбора и многоальтернативности решений необходимо включить в сформированный перечень услуг и продуктов как основные средства защиты: антивирусное программное обеспечение, DLP-системы, межсетевые экраны, системы обнаружения вторжений, комплексы фильтрации трафика, системы резервного копирования и пр. – так и сопутствующие средства: источники бесперебойного питания, системы видеонаблюдения и пр.

4) Управление инцидентами. Менеджмент инцидентов ИБ обеспечивает своевременную и эффективную модернизацию существующей системы защиты на основе полученных ранее данных о ее недостатках и достоинствах. Управление инцидентами связано с процессом обработки и анализа данных о работе системы защиты, сравнения полученных сведений в результате её эксплуатации с исходными и плановыми показателями.

При проектировании деловой игры необходимо разработать систему оценивания построенной участниками защиты, базирующуюся на оценке её эффективности, а также логике реализации угроз и принципах действия выбранной системы защиты. Для выполнения данного условия целесообразно вводить числовые характеристики для последующих расчетов и предоставления результатов участникам.

К таким числовым величинам можно отнести вероятность реализации угроз, размер потенциальных потерь в случае их реализации, показатель защиты СрЗИ от конкретной угрозы.

Для описания вероятности реализации угроз может быть использована аналогия с Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных ФСТЭК России.

Вводятся четыре вербальных градации этого показателя:

- маловероятно – отсутствуют объективные предпосылки для осуществления угрозы;
- низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию угрозы;
- средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности недостаточны;
- высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности не приняты.

Каждой позиции вероятности задано числовое значение в соответствии с таблицей 2, которое используется в качестве расчётного значения при определении показателя необходимой защищенности.

Для описания степени потенциальных потерь могут быть заданы числовые значения, равные денежному ущербу в игровой валюте, представля-

Таблица 2

Числовые характеристики вероятностей угроз

№	Наименование оценки вероятности	Расчетное значение (Pi)
1	Маловероятна	0
2	Низкая вероятность	0,3
3	Средняя вероятность	0,5
4	Высокая вероятность	0,8

ющие собой данные известных случаев реализации угроз или рассчитанные приближенно.

Также в рамках проведения деловой игры необходимо реализовать процесс изучения участниками вариантов поведения сформированной системы защиты в реальных условиях за счет формулирования кейсов реализации угроз с целью повышения ценности получаемого профессионального опыта.

Для осуществления данного этапа представляется возможным разработать кейсы реальных инцидентов, основанные на данных судебных практик или открытых сведений компаний о реализации рассматриваемых угроз, а также теоретических сведений о построении системы защиты. Для этого необходимо разработать конкретную ситуацию и предусмотреть вероятные последствия ее реализации исходя из потенциально возможных вариантов построения системы защиты.

Пример разработки кейса приведен на рисунке 3 с описанием вероятных последствий в зависимости от выбранных участниками СрЗИ от наихудшего к наилучшему.

Таким образом, проектирование деловых игр по комплексному управлению ИБ сопровождается моделированием всех этапов процесса построения КСЗИ на предприятии. В процессе проведения игры требуется не только обеспечить работу обучающихся с конкретными средствами и методами защиты, но и создать условия для интеграции знаний и навыков в профессиональные ситуации, приближенные к реальным условиям современного бизнеса.

Для повышения ценности получаемого обучающимися опыта необходимо предусмотреть

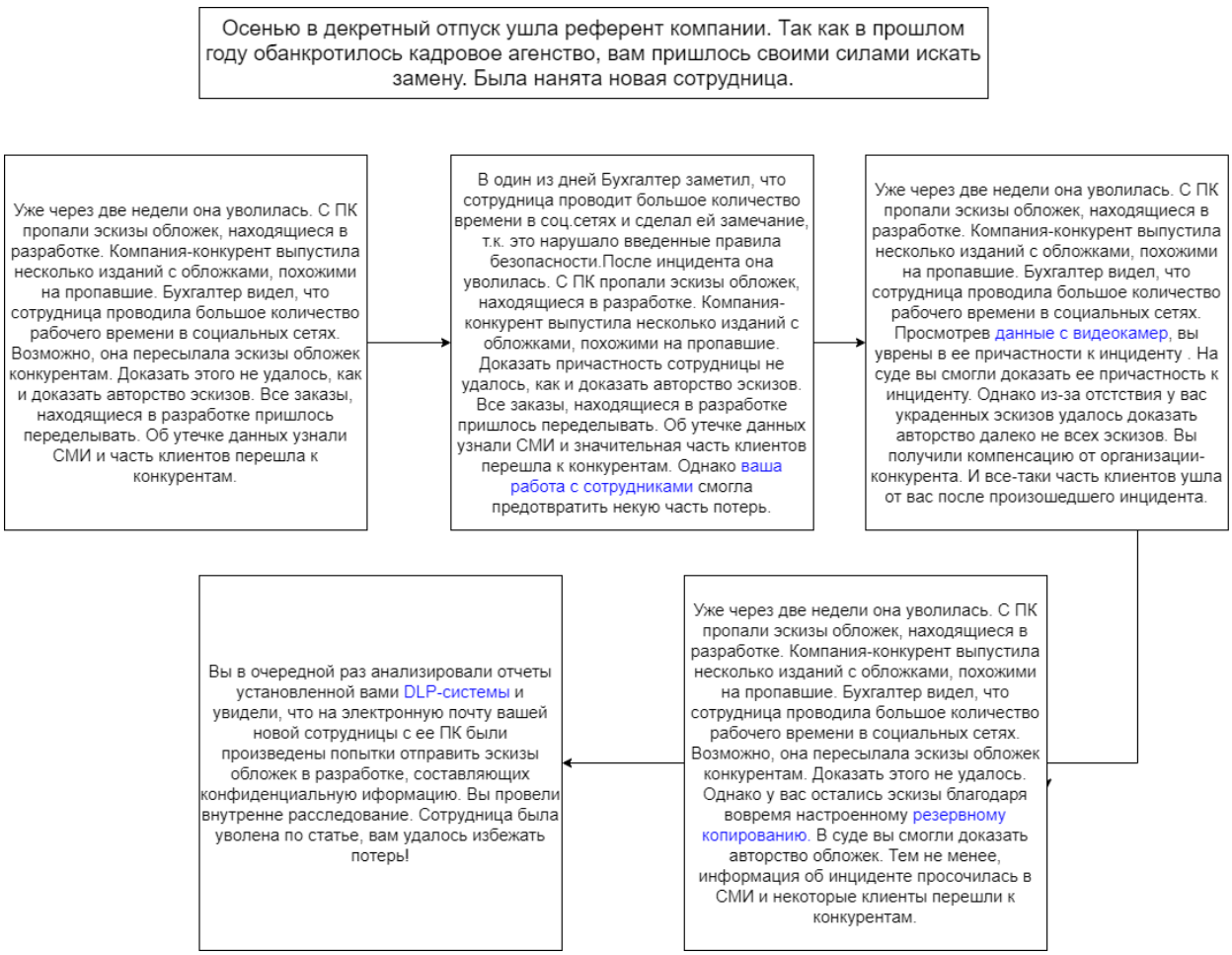

Рисунок 3 – Разработка кейса деловой игры

постановку конкретной профессиональной задачи, предоставление полной и достаточной информации о моделируемом экономическом субъекте и его характеристиках для обеспечения корректной оценки рисков и последующего построения системы защиты а также ее объективную всестороннюю оценку.

Список литературы

1. *Федоров Д.Ю., Стельмашонок Е.В.* Компетенции Ворлдскиллс, трудовые функции профстандартов и повышение качества образования студентов в области защиты информации // Конвергенция цифровых и материальных миров: экономика, технологии, образование. Сборник научных статей международной научной конференции. 21–22 июня 2018 г. Санкт-Петербург. Conference of St.-Petersburg State University of Economics. / Под ред. проф. В.В. Трофимова, В.Ф. Минакова. – СПб.: Изд-во СПбГЭУ, 2018. – С. 269-273

2. Информационная безопасность цифрового пространства: коллективная монография / Под ред. Е.В. Стельмашонок, И.Н. Васильевой. – СПб.: Изд-во СПбГЭУ, 2018. – 160 с.

3. *Подружкина Т.А., Федоров Д.Ю.* Проблемные вопросы подготовки кадров в области информационной безопасности в условиях стандартизации профессиональной деятельности // Информационная безопасность регионов России (ИБРР-2015): матер. IX Санкт-Петербургской межрегион. конф., Санкт-Петербург, 28-30 октября 2015 г. – СПб.: СПОИСУ, 2015. – С. 349-350.

4. *Бельчиков Я.М., Бирштейн М.М.* Деловые игры – Рига: АВОТС, 1989 – с. 304

5. *Колесникова Д.С., Рудниченко А.К.* Требования к разработке автоматизированной обучающей системы в области информационной безопасности [Электронный ресурс] / Инженерный вестник Дона, №1 (2019). – Режим доступа http://www.ivdon.ru/uploads/article/pdf/IVD_140_kolesnikova_rudnichenko.pdf_8b17039bfd.pdf, свободный

Статья поступила в редакцию 12 мая 2020 г.
Принята к публикации 29 июня 2020 г.

Ссылка для цитирования: Федоров Д.Ю., Верзилова А.С., Хорошенко В.С., Буйневич М.В. Этапные компоненты деловых игр при обучении студентов построению комплексной системы защиты информации // Национальная безопасность и стратегическое планирование. 2020. № 2(30). С. 43-49. DOI: https://doi.org/10.37468/2307-1400-2020-2-43-49