DOI 10.36622/VSTU.2023.26.1.001
УДК 004.056

КИБЕРПОЛИГОН КАК ПРОЕКТ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ

Г.А. Остапенко, В.И. Белоножкин, А.А. Остапенко, М.Е. Волкова

В работе рассматривается проект создания киберполигона в качестве тренажера тестируемых систем на предмет управления рисками успешности реализации сетевых атак. В этой связи обсуждаются принципы оценки и регулирования рисков от университетской подготовки специалистов до их тренингов условиях создаваемого полигона. Предлагается соответствующий глоссарий и рассматриваются предпосылки для полигонной организации. При этом, киберсистема определяется как социо-техническая сущность, в которой полигоном эмулируется процесс информационного противоборства. В этой связи, формулируются задачи построения киберполигона, оценивается их инновационность. Впервые описываются области возможного сотрудничества университета и IT-предприятий в вопросах построения киберполигона, а также – мотивы инновационной интеграции участников проекта.

Ключевые слова: киберсистема, киберполигон, информационные риски, эмуляция, инновация.

Введение

Увы, воинствующие либерал демократы во многом осквернили отечественное образование, что существенно осложняет подготовку кадров в области кибербезопасности [1-7].

Однако, тем более интенсивнее надо внедрять в их студенческое сознание адекватное мироощущение. Концентрация на критических аспектах в этом вопросе позволяет во многом устранять имеющие место проблемы. Опыт заточки курсового проектирования и практик под проблематику обеспечения безопасности показал на нашей кафедре, что на четвером курсе мы в основном имеем студентов, способных самостоятельно решать профессиональные задачи с использованием аппарата риск-анализа.

Тем более, что мы сейчас участвуем в разработке четвертого поколения образовательного стандарта, где планируется в специалитете шестилетнее образование с возможностью присвоения двух квалификаций. Одна из них может быть по управлению рисками, в том числе с помощью машинного обучения.

Задача перевода с человечьего языка на машинный (т.е. программирования) будет стоять всегда. Разговор идет о том, что такую подготовку следует адаптировать под проблематику обеспечения безопасности и устойчивого развития киберсистем на всех стадиях их жизненного цикла от создания до эксплуатации.

Мало того, и не программистские ИБ-специальности надо подчинять необходимости создания программных продуктов в курсовом и дипломном проектировании. Инструментарием автоматизации решения своих профессиональных задач должны владеть все IT-ишники.

Чем инновационее приобретенное знание, тем нестерпимее оно требует своего широкого распространения, опережающего даже экономический интерес.

Через студенческий учебный процесс, в необходимой степени технически оснащенный, такая диффузия инноваций наиболее эффективна.

Здесь и надо искать университетский и национальный интерес в формировании культуры риск-анализа киберпространства [1-7].

Погружаясь все глубже в проблематику обеспечения кибербезопасности, все отчетливее начинаешь понимать, что её сущность состоит не только и не столько в парировании кибератак, а в необходимости

формирования культуры управления рисками на всех стадиях жизненного цикла киберсистем от их проектирования до применения.

В этом отношении площадка создания киберполигона могла бы стать весьма продуктивным пространством взаимодействия и сотрудничества университета и IT компаний для тренинга своих идей и продуктов в условиях нарастающих информационных угроз. В этом и состоит университетский и, надеюсь, не только интерес.

При этом логично было бы встроиться в любую продвинутую платформу, разделяющую нижеприведенный методический подход.

При этом, думается, наиболее органичной будет коллегиальная координация проекта со стороны всех его участников.

Народная инновация пусть принародно и регулируется!

Увы, многие адаптированные у нас западные методики риск-анализа нацелены на вычисление некоторого магического числа.

Однако, полноценно характеризовать одним числом возможно только одну сущность – это бесконечность!

Риск же есть дискретная функция, прежде всего зависящая от величины ущерба, и не только.

Отсюда регулирование риском – в сущности весьма непростая задача, ибо уменьшая его в одном диапазоне ущербов, мы неизбежно повышаем значения риска в других диапазонах. Свести риск до нуля можно только уничтожив систему.

Поэтому управление функцией риска — это далеко не вариация одним числом, а многопараметрическая оптимизация на всем жизненном цикле системы. Именно этому посвящены наши теоретические и практические усилия.

По большому счету, чисто риск-оценка не является исчерпывающей. Такое допустимо лишь при стабильных шансах полезности системы.

Достаточно вспомнить крылатые фразы картежников: «Игра не стоит свеч» и «Кто не рискует, тот не пьет шампанского». Они говорят о том, что риск ущербности и шанс полезности должны соответствовать друг другу.

Отсюда вытекает интегральная оценка, которая в простейшем варианте может выражаться в разности значений этих двух функций. При этом, оси пользы и ущерба должны быть сведены в одну, относительно которой ведутся соответствующие сравнения.

Так можно найти шансо-риск и, по большому счету, проблема состоит в том, чтобы создать регулярные методы система систем с заданным шансориском.

Такая междисциплинарная наука рано или поздно обязательно появится, где уместно рассмотреть приемственность методолгии оптимального синтеза систем, но уже с заданными характеристикам полезности и ущербности.

Предпосылкой для создания киберполигона можно считать следующие наработки:

1. По блоку актуализации данных имеется программный модуль автоматизированного выявления и риск-оценки уязвимостей программного обеспечения. В нем используется аналитическая визуализация на основе информационных карт.

2. По блоку эмуляции разработано, эксплуатируется и развивается программное обеспечение, осуществляющее риск-моделирование эпидемических процессов в сетевых структурах киберпространства.

3. Успешно функционирует модуль, автоматизировано выявляющий локализацию и деструктивность контентов в социальных сетях для заданного контингента сотрудников или учащихся организации.

4. Вводится в эксплуатацию модуль, выявляющий эмоциональные состояния персонала киберсистем.

Вышеперечисленные продукты активно используются в учебной среде.

Глоссарий

Киберсистема – социотехническая система, под управлением своего персонала, с помощью имеющегося в её распоряжении аппаратного и программного обеспечения осуществляющая генерацию, передачу, хранение и защиту информации.

Безопасность киберсистемы – состояние

её защищенности от информационных угроз, риск реализации которых не превышает допустимых значений.

Риск – возможность наступление ущерба.

Информационный риск – возможность наступления ущерба в информационной сфере.

Мера риска – величина ущерба, помноженная на вероятность её наступления.

Эмуляция – комплекс информационно-технических средств, предназначенный для копирования функций одной вычислительной системы на другую таким образом, чтобы эмулированное поведение как можно ближе соответствовало поведению оригинальной системы.

Киберполигон – программно-техническое учебно-тренировочное устройство, искусственно эмулирующее поведение исследуемой киберсистемы в условиях воздействия различных информационных угроз.

Инновация – нововведение или новшество, обеспечивающее повышение эффективности процессов и качества продукции, востребованное рынком и соответствующее актуальным социо-экономическим и культурным потребностям общества.

Основы оценки регулирования рисков

1. Риск является функцией ущерба в его дискретных значениях, где:

$Risk(v_i) = v_i \times P(v_i)$, $i = 1, 2, \ldots$

v_i – взаимно исключающие события и $\sum_i P(v_i)=1$, где P – вероятность появления ущерба значения v_i.

2. Применение вместо P плотности вероятности φ недопустимо. Здесь нужно φ дискретизировать по значениям ущерба, иначе нарушается размерность риска.

3. Перемножение ущербов также ошибочно из-за нарушения размерности риска.

4. Выбор того или иного вида распределения не может быть «делом вкуса проектанта». Здесь требуется (по данным статистики) доказывать справедливость выдвинутой гипотезы по всем канонам теории вероятностей.

5. Риск-анализ успешности сложных атак следует осуществлять при установлении независимости или взаимозависимости (особо сложный случай, рассматриваемый через условные вероятности) ожидаемых ущербов. Слепое суммирование или перемножение значений рисков недопустимо.

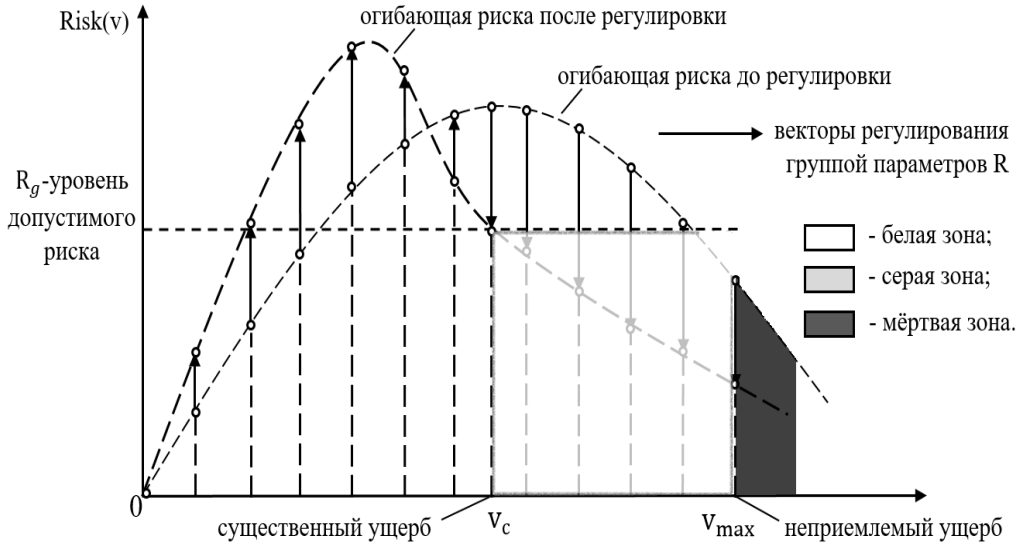

Рис. 1. Управление функциями риска

Пусть Risk(C, R) – функция риска, определенная ранее, где:

C – группа параметров, неуправляемых администрацией атакуемой сети (интенсивность атак, количество атакуемых её элементов и т.п.);

R – группа параметров, регулируемых администрацией сети (вероятность успеха единичной атаки, средний ущерб от единичной успешной атаки и т.п.).

Задача регулирования состоит в том, чтобы подобрать значения параметров R таких, чтобы в заданном диапазоне ущербов (v_c, v_{max}) значения риска не превышали допустимого уровня R_g.

Регулировка несколькими параметрами из множества R, как правило, реализуется автоматизировано с помощью оптимизационных алгоритмов.

При этом надо понимать, что, уменьшая риск в одном диапазоне ущербов, мы неизбежно увеличиваем его в других диапазонах v. Это (рис.1) делается осознанно:

– в диапазоне (v_c, v_{max}), критическом для нас, его обязательно надо понижать;

– при этом в диапазоне малых (незначительных для нас) ущербов мы допускаем рост риска, который неизбежен, в нашем случае, согласно теории вероятностей.

Таким образом, задавая в своей работе (обязательно обоснованно) параметры функции риска R_g, v_c и v_{max} и определившись с множеством варьируемых параметров риска R, мы можем приступать к оптимизационным процедурам. Когда таких параметров имеется не более 3-х, оптимизационные алгоритмы работают довольно эффективно.

Относительно оси ущербов, иногда прибегают (в целях ухода от размерностей) к нормированию по v_{max}. Тоже самое возможно сделать для оси риска через нормирование по R_g.

Следуя вышеуказанным рекомендациям, можно организовать нужное управление рисками, где возможно следующее решение через аналитическое выражение функции риска (на стадии риск-анализа определенное), когда мы получаем управление

$$Risk(C, R) = R_g,$$

т.е. $$Risk(C, R) = P(C, R)\, v_c = R_g$$

или $$P(C, R) = \frac{R_g}{v_c}.$$

Это уравнение имеет несколько переменных и его решение очевидно затрудненно. Однако, если задать группу параметров C (на основе опыта защиты подобных систем), то можно преступать к подбору R – параметров, удовлетворяющих уравнени. Когда множество R состоит лишь из одного варьируемого параметра, задача сведется к поиску единственного решения нелинейного уравнения.

Уместно также обратить внимание на обоснованность выборы параметра v_c. Здесь наряду с чисто техническим аспектом (допустимость утраты информационных блоков или отказов в обслуживании атакуемой системы) возможно и относительно абстрактное сопоставление мощностей «белой» S_0' и «серой» S_1' зон под графиком риска (рис.1), где:

$$S_0' = \sum_0^n Risk(v) \text{ при } n = \frac{v_c}{\Delta U};$$

$$S_1' = \sum_n^m Risk(v) \text{ при } m = \frac{v_{max}}{\Delta U}.$$

Где ΔU – шаг дискретизации риска.

Здесь участвуют частоты успешности атак и наносимых ими ущербов, характеризующих результаты регулирования риска.

При этом, следует обратить внимание на следующие возможные ошибки и сложности:

1. Попытка оценить вероятность успеха атаки через произведение некоторых коэффициентов

$$P(v) = \prod_i K_i:$$

– во-первых, утрачивает зависимость от величины ущерба v, что принципиально не допустимо для риск-анализа:

$$v_1 \rightarrow P(v_1) \rightarrow Risk(v_1) = v_1 \times P(v_1);$$
$$v_2 \rightarrow P(v_2) \rightarrow Risk(v_2) = v_2 \times P(v_2);$$
$$\cdot$$
$$\cdot$$
$$\cdot$$
$$v_{max} \rightarrow P(v_{max}) \rightarrow Risk(v_{max}) = v_{max} \times P(v_{max});$$

– во-вторых, создает дополнительные проблемы для проектировщика в части практического определения значений коэффициентов K_i (как правило таких статданных в открытом доступе не найти).

2. Подобная ошибка встречается также, когда ущерб пытаются оценить через произведение коэффициентов R_i, характеризующих важность атакуемого узла

$$v = \prod_i R_i.$$

Здесь теряется связь со спецификой атаки, которая и задает собственно значения ущербов $\{v_1, v_2, \ldots, v_{max}\}$. Так, для атаки «отказf в обслуживании» первостепенную роль играет время простоя узла, с которым утрачен доступа к информации. В свою очередь, для атаки «нарушения целостности

информации» ущерб будет определяться количеством утраченных узлом информационных блоков. Легко заметить, что важность узла (заданная через коэффициенты R_i) прямо не связана с вышеуказанными параметрами, задающими значения искомого ущерба.

К тому же, важность узла, оцененная через топологию сети (метрики R_i), весьма однобока, ибо не учитывает трафик наполнителя (информации) сети, протекающего через рассматриваемый узел.

3. Конструирование выражения риска через произведение или сумму формул вероятностей – очень сложная задача, решение которой требует глубокой аналитики на каждом этапе реализации сценария (вектора) атаки и стыковки дискретных функций вероятностей (полученных для вышеупомянутых этапов) по шагам дискретизации ущерба и т.п. для выполнения операций над значениями вероятностей. Это насколько почетная, настолько архи-трудная задача риск-синтеза (безответственно её решать не стоит).

4. Применение функций плотности вероятности φ (через выдвижение и доказательство соответствующей гипотезы) с помощью шага дискретизации ΔU ущерба позволяет найти вероятность

$$P(v) = \Delta U \times \varphi (A, v),$$

где A - множество параметров распределения.

Это возможно осуществить при наличии статистических данных об ущербах и частоты их наступления в объекте исследования (это не так просто найти). При этом, возникают весьма существенные трудности выявления параметров системы (объекта), регулировкой которых можно целенаправленно (по разработанному алгоритму) однозначно управлять множеством параметров распределения A (иначе все будет тщетно).

Контекст информационного риск-анализа

Все (без исключения) системы рождаются, живут и исчезают в борьбе с рисками, величина которых задает траекторию их существования (его величество риск-вездесущ).

В киберпространстве особую значимость имеют информационные риски, которые преследуют киберсистемы не только при отражении атак (управление рисками необходимо на всех стадиях жизненного цикла от создания до штатной эксплуатации).

Киберсистема – есть социотехническая сущность (даже максимально расчеловеченные средства искусственного интеллекта способны нанести неприемлимый социальный ущерб).

Киберполигон – есть инструментарий оценки и регулирования рисков ущербности, а также – шансов достижения требуемой полезности исследуемой системы (шансориск становится интегральным критерием).

Концепт проекта

Создаваемый киберполигон ориентирован на тренинг тестируемых систем в их технической и кадровой составляющих посредством эмуляции процессов реализации информационных рисков и их регулирования.

Отсюда вытекают следующие задачи:

1. Создание автоматизировано актуализируемых баз данных и знаний об угрозах, уязвимостях, сценариях (векторах) атак и рисках их успешной реализации в отношении киберсистем.

2. Построение риск-эмуляторов, копирующих функции тестируемых киберсистем в контексте возможных нарушений их безопасности, оцениваемых через информационные риски.

3. Создание средств интеллектуальной поддержки технических и организационных решений по управлению информационными рисками в тестируемых киберсистемах на стадиях их создания и эксплуатации.

Заключение

Инновационность проекта. Впервые среди решений данного профиля задач вводится автоматизация (в режиме реального времени) актуализация данных и знаний об информационных вредоносах (используемых уязвимостях, векторах атак, рисках их успешной реализации). Тем самым обеспечивается постоянная боеготовность полигонных служб к новым вызовам.

Принципиальным отличием от аналогов следует считать учет не только информационно-кибернетических, но и информационно-психологических рисков (человеческого фактора – весьма значимого для обеспечения кибербезопасности)

нарушения безопасности.

На основе искусственных нейросетей предполагается обеспечить интеллектуальную поддержку решений по управлению информационными рисками исследуемых систем, включая возможность активной их защиты.

Предлагается начать это необратимое движение с подключения работодателей к созданию Полигона в качестве тренажера для студентов вуза и персонала предприятий, учитывающего как технический, так и человеческий факторы оценки и регулирования информационных рисков. Столь широкая народная интеграция инноваций значительно расширит возможности эффективной коммуникации учащихся и трудящихся в предлагаемом пространстве.

При этом, на стыке научных и технических школ региона от штамповки программистов удается перейти к игре в долгую по формированию культуры управления информационными рисками, без которой принципиально невозможно создавать интеллектуально развитые и надежно защищенные киберсистемы (другие не нужны в условиях войны).

Области возможного сотрудничества. Опыт региональных IT – организаций, приобретённый в борьбе с кибер-вредоносами, представляется целесообразным использовать для машинного обучения блока интеллектуальной поддержки управления информационными рисками. Здесь вполне возможен мультипликативный эффект от использования аккумулированных знаний и данных, полученных от практиков – участников проекта, в том числе при организации активной защиты от угроз.

На платформах партнеров проекта целесообразна отработка его модулей в решении практических задач оценки и регулирования информационных рисков. В этом случае по запросам партнеров возможна организация текущего противодействия как информационно-кибернетическим, так и информационно-психологическим угрозам.

Мотивы инновационной интеграции. Инициированное кибердружиной ВГТУ создание Полигона можно рассматривать в качестве народной инновации, направленной на воспроизводимые компетенции, представленные в масштабе профессионального сообщества на базе университета. Через народную инновацию рождалась Силиконовая долина, и только потом в университетскую среду внедрились малые компании, а позднее и транснациональные корпорации.

Поэтому ВГТУ, как катализатор народного творчества, имеет все возможности стать в регионе центром притяжения молодых инноваторов, генерирующих технологически оригинальные и масштабные идеи. Здесь массово создаются точки присутствия, распространяются компетенции, реализуются обучение и тренинг специалистов. При этом, особую ценность представляют специалисты с навыками управления. В случае с Полигоном это компетенции управления информационными рисками в контексте обеспечения безопасности социо-технических систем, лежащих в основе современного киберпространства

Университет здесь выступает питательной учебно-научной средой, инкубационно взращивающей подобные кадры и стартапы. С учетом актуальности импортозамещения и дефицита специалистов, эффективно управляющих кибербезопасностью, наступает время, когда региональные IT – предприятия от рекламно-потребительской кадровой политики должны перейти к активному участию в работе вышеуказанного инкубатора инновационных специалистов.

При этом, на стыке научных и технических школ региона от штамповки программистов удается перейти к игре в долгую по формированию культуры управления информационными рисками, без которой принципиально невозможно создавать интеллектуально развитые и надежно защищенные киберсистемы (другие не нужны в условиях войны).

В качестве жеста доброй воли Университет может:

1. Организовать для участников Полигона учебный курс по основам риск-анализа (см. Приложение);

2. Предоставить возможность

публикации в журнале «Информация и безопасность» результатов научно-практической деятельности по тематике Полигона;

3. Предоставить возможность авторского участия в коллективных монографиях серии «Теория сетевых войн», публикуемых издательством «Горячая линия – Телеком» по тематике Полигона.

Координацию деятельности по созданию Полигона целесообразно осуществлять с помощью экспертного совета, в состав которого уместно включить полномочных представителей участников проекта.

Список литературы

1. Эпидемии в телекоммуникационных сетях / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2017. – 284 с. (Серия «Теория сетевых войн»; вып. 1).

2. Атакуемые взвешенные сети / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2017. – 284 с. (Серия «Теория сетевых войн»; вып. 2).

3. Социальные сети и деструктивный контент / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2017. – 284 с. (Серия «Теория сетевых войн»; вып. 3).

4. Социальные сети и риск-мониторинг / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2019. – 284 с. (Серия «Теория сетевых войн»; вып. 4).

5. Социальные сети и психологическая безопасность / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2020. – 284 с. (Серия «Теория сетевых войн»; вып. 5).

6. Сетео-информационная эпидемиология / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2021. – 284 с. (Серия «Теория сетевых войн»; вып. 6).

7. Картография защищаемого киберпространства / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2022. – 372 с. (Серия «Теория сетевых войн»; вып. 7).

Финансовый университет при Правительстве Российской Федерации
Financial University under the Government of the Russian Federation

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 23.02.23

Информация об авторах

Остапенко Григорий Александрович – д-р техн. наук, проректор Финансового университета при Правительстве Российской Федерации, e-mail: mnac@comch.ru

Белоножкин Владимир Иванович – д-р техн. наук, профессор Воронежского государственного технического университета, e-mail: mnac@comch.ru

Остапенко Александр Алексеевич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Волкова Марина Евгеньевна – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

CYBERPOLYGON AS A PROJECT OF INFORMATION RISK MANAGEMENT

G.A. Ostapenko, V.I. Belonozhkin, A.A. Ostapenko, M.E. Volkova

The paper considers the project of creating a cyberpolygon as a simulator of tested systems for managing the risks of successful implementation of network attacks. In this regard, the principles of risk assessment and management are discussed from the university training of specialists to their training under the conditions of the created test site. A related glossary is proposed and prerequisites for a landfill organization are considered. At the same time, the cyber system is defined as a socio-technical entity in which the process of information confrontation is emulated by a testing ground. In this regard, the tasks of building a cyberpolygon are formulated, their innovativeness is assessed. For the first time, the areas of possible cooperation between the university and IT enterprises in the construction of a cyberpolygon are described, as well as the motives for the innovative integration of project participants.

Keywords: cybersystem, cyberpolygon, information risks, emulation, innovation.

Submitted 23.02.23

Information about the authors

Grigory A. Ostapenko – Dr. Sc. (Technical), Vice-Rector of the Financial University under the Government of the Russian Federation, e-mail: mnac@comch.ru

Vladimir I. Belonozhkin – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: mnac@comch.ru

Alexander A. Ostapenko – student, Voronezh State Technical University, e-mail: mnac@comch.ru

Marina E. Volkova – student, Voronezh State Technical University, e-mail: mnac@comch.ru