Федеральное государственное автономное образовательное учреждение высшего образования «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»
Институт радиоэлектроники и информационных технологий – РТФ
Учебно-научный центр «Информационная безопасность»

На правах рукописи

Макарова Ольга Сергеевна

РАЗРАБОТКА МЕТОДИКИ ПРОГНОЗИРОВАНИЯ ДИНАМИКИ ИЗМЕНЕНИЯ ВЕКТОРА КОМПЬЮТЕРНОЙ АТАКИ С ТОЧКИ ЗРЕНИЯ НАРУШИТЕЛЯ

2.3.6 Методы и системы защиты информации,
информационная безопасность

ДИССЕРТАЦИЯ
на соискание ученой степени кандидата
технических наук

Научный руководитель:
доктор технических наук, профессор
Поршнев Сергей Владимирович

Екатеринбург - 2021

Оглавление

ВВЕДЕНИЕ

Актуальность темы исследования и степень ее проработанности

Защита информации (ЗИ) предусмотрена Статьей 16 Федерального закона (ФЗ) от 27.07.2006 «Об информации, информационных технологиях и о защите информации» [1], а также иными нормативно-правовыми актами, разработанными государственными регуляторами в области информационной безопасности (ИБ). Данные документы предусматривают применение типовых наборов методов и средств ЗИ, сформированных на базе типовых моделей угроз ИБ, созданных ФСТЭК России и ФСБ России [2, 3, 4]. При этом действующим законодательством предусмотрена возможность дополнения перечня актуальных угроз ИБ новыми моделями угроз (МУ) [5, 6, 7, 8]. В соответствие с «Методикой определения угроз БИ», разработанной ФСТЭК России [5], оценка угроз ИБ осуществляется с помощью метода экспертных оценок.

Международные стандарты [9–17] для оценки угроз ИБ предлагают использовать:

- методологию *IT-Grundschutz*, которая, в одних случаях, рекомендует использовать в организациях и информационных системах (ИС) набор мер ЗИ, состав которого определен на основе сценариев негативных последствий для активов организации, в других, также использовать дополнительный перечень мер ЗИ, формируемых экспертным путем;
- методологию *ISO* 2700x, рекомендующую формировать набор требований по ЗИ на основе оценки рисков ИБ, которая осуществляется экспертным путем в соответствии с внутренним положением организации по оценке рисков ИБ (при этом, ответственность за принятие рисков в целом несет руководитель организации (владелец активов)).

Необходимо отметить, что метод экспертных оценок, которому, как показывает практика ИБ, присущ ряд ограничений (в том числе: субъективность; отсутствие полноты или избыточность; сложная повторяемость процесса) не обеспечивает формирования исчерпывающего перечня мер по ЗИ. При этом, очевидно, что данный метод предназначен для получения оценок угроз ИБ в

конкретный момент времени, но не для их прогнозирования в последующие моменты времени.

В этой связи были предприняты многочисленные попытки модернизации действующих международных стандартов и нормативно-правовых документов в области обеспечения ИБ с целью автоматизации процесса формирования профилей ЗИ, использования соответвующих методов визуализации, повышения эффективности экспертной оценки, а также специальных методов ее проведения [18-31]. Необходимо отметить, что оценки угроз и рисков ИБ в данных работах проводились, исключительно, с точки зрения организации/владельца актива. Кроме того, в большинстве этих работ авторы даже не пытались оценивать эффективность и практическую применимость, предложенных ими изменений.

Также отметим, работы [32–35], в которых проведен анализ контента форумов *DarkNet*, в первую очередь, информации об инцидентах ИБ, вновь разрабатываемых и/или уже известных и активно обсуждаемых на форумах *DarkNet* методах компьютерных атак (КА), с целью прогнозирования соответствующих векторов КА с учетом частоты их упоминаний, а также эмоциональной окраски обсуждений. Данные работы, с нашей точки зрения, следует рассматривать, как первые попытки учета информированности нарушителя о методе проведения КА при оценке угроз ИБ, однако, не завершившиеся созданием рекомендаций по оценке целесообразности проведения КА с точки зрения нарушителя. В этой связи использование информации, извлекаемой из форумов *DarkNet* для прогнозирования векторов КА осталась низкой.

Эффективность прогнозов новых уязвимостей программного обеспечения (ПО) с помощью методов одинарного, двойного и тройного экспоненциального сглаживания [36-38], статистических методов (Кростона, *ARIMA*) [35, 36, 39, 40], кластерного анализа [41, 42], нейронных сетей [36, 43] и машинного обучения [36, 43, 44], основанные на анализе накопленной информации о количестве уязвимостей и их типах в предыдущих версиях, а также и векторов КА, основанных на анализе частоты упоминаний методов КА за определенные

временные периоды в *DarkNet* [35], оказались не эффективными, так как существенно расходятся с реальными данными.

При этом необходимо отметить, что данные методы позволяют получать оценки уязвимостей исключительно с точки зрения атакующей стороны. В тоже время в экономической и финансовых сферах, а также в области предупреждений преступлений общей практики накоплен положительный опыт применения для анализа экономических мотивов преступников «Теории положений о криминологии» (ТПК) Ч. Беккариа и И. Бентама [45–47], которая, однако, при оценке вероятностей КА ранее не использовалась. В этой связи разработка подходов для оценки угроз ИБ с учетом экономических интересов нарушителя является актуальной.

Цель диссертационного исследования состоит в научно обоснованной разработке метода оценивания с точки зрения нарушителя вероятностей проведения успешных КА и прогнозирования динамики их изменения во времени.

Для достижения поставленной цели сформулированы и решены следующие **задачи**:

1. Анализ нормативно-правовой базы, регламентирующей подходы к оценке угроз ИБ, и научных подходов, используемых для определения и прогнозирования КА.

2. Разработка и обоснование базовых принципов и подходов к построению математической модели оценки вероятности реализации нарушителем КА и математической модели, описывающей динамику изменения вектора КА во времени, построенного с точки зрения нарушителя.

3. Разработка методики прогнозирования динамики изменения вектора КА, основанной на использовании предложенных математических моделей, и подтверждение ее работоспособности.

Объект исследования: математические методы и модели анализа и прогнозирования КА.

Предмет исследования: методы оценивания с точки зрения нарушителя вероятностей проведения успешных КА, математические модели, описывающие динамику КА, обеспечивающие прогнозирование векторов вероятных КА.

Научная новизна работы заключается в разработке научно обоснованных:

1. математической модели оценки вероятности реализации нарушителем КА и идентификации ее параметров, основанной на положениях ТПК (соответствует п. 7 паспорта специальности);

2. математической модели, описывающей динамику возможности реализации нарушителем КА во времени, и идентификации ее параметров, основанной на положениях Теории диффузии инноваций (ТДИ) (соответствует п. 14 паспорта специальности);

3. методики прогнозирования динамики векторов КА, построенной с точки зрения нарушителя (соответствует п. 15 паспорта специальности).

Практическая и теоретическая значимость работы заключается в:

1. обосновании целесообразности применения ТПК для разработки математической модели принятия решения нарушителем о проведении КА;

2. обосновании целесообразности использования ТДИ, развитой в работах Э. Роджерса [48], Ф. Басса [49], Э. Мэнсфилда [50] и Т. Хагерстранда [51], для построения математической модели, описывающей динамику изменения вектора КА во времени;

3. обоснованном выборе набора источников информации, обеспечивающих идентификацию параметров разработанных моделей;

4. подтверждении адекватности методики прогнозирования динамики векторов КА с точки зрения нарушителя, позволяющая выявлять тренды развития КА.

Методология и методы исследований. В работе использованы математическое моделирование, методы системного анализа, ТПК, ТДИ.

Основные положения, выносимые на защиту

1. На основе ТПК построена математическая модель принятия решения нарушителем о проведении КА, адекватность которой подтверждена результатами

анализа КА, реализованной с помощью вредоносного программного обеспечения (ВПО) *Petya*, а также результатами натурного моделирования КА с помощью программно-аппаратного комплекса (ПАК) «*Ampire*».

2. На основе ТПК и ТДИ построена математическая модель динамики распространения КА, адекватность которой подтверждена результатами анализа динамики КА, реализованной с помощью ВПО *WannaCry*.

3. На основе построенных математической моделей принятия решения нарушителем о проведении КА и математической модели, описывающей динамику распространения КА, разработана методика прогнозирования динамики изменения вектора КА, адекватность которой подтверждена согласованностью результатов прогнозирования вектора КА в 2019 г. с помощью данной методики с результатами анализа доступной статистической информации об успешно реализованных КА в 2019 г.

Достоверность полученных результатов обеспечивается использованием известных математических методов, адекватных задачам исследования, а также согласованностью оценок КА, полученных с помощью предложенных моделей и методики, с результами анализа известных КА и результатами натурного моделирования КА, проведенного с помощью ПАК «*Ampire*».

Внедрение результатов диссертационного исследования. Результаты диссертационного исследования используются в федеральном государственном автономном образовательном учреждении высшего образования «Уральский федеральный университет им. Первого Президента России Б.Н. Ельцина» (акт об использовании № 33.02-32/230 от 20.08.2021), Акционерным обществом «Перспективный мониторинг» (акт об использовании № ИПМ-2021-0104 от 23.08.2021).

Апробация работы. Основные результаты работы докладывались на следующих научных конференциях:

1. III Международной студенческой научной конференции «Инновационные механизмы управления цифровой и региональной экономикой», 17.06-18.06.2021, Москва, 2021.

2. Международной научной конференции *Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, 13.05-14.05.2021, Екатеринбург, 2021.

3. Международной научно-технической конференции «Автоматизация», 6.09-12.09.2020, Сочи, 2020.

4. Международной научной конференции *Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, 14.05-15.05.2020, Екатеринбург, 2020.

5. I Международная научая конференция «Технические науки: проблемы и перспективы», март 2011, Санкт-Петербург, 2011.

Личный вклад. Автор обосновал возможность прогнозирования динамики векторов КА с точки зрения нарушителя во времени на основе данных из общедоступных источников информации о КА получив практически подтвержденные результаты оценки. Разработал научно обоснованные математические модели определения ожидаемой полезности от КА и динамики возможности реализации КА во времени с точки зрения нарушителя.

Публикации. По теме диссертации опубликовано 10 научных работ, в том числе 6 научных статей в изданиях, определенных ВАК РФ и Аттестационным советом УрФУ, из них 2 в изданиях, индексируемых в международных цитатно-аналитически базах *Scopus* и *Web of Science*.

Объем и структура работы. Диссертация состоит из введения, 3 глав, заключения и 8 приложений. Полный объем диссертации составляет 218 страниц, включая 26 рисунков и 25 таблиц. Список литературы содержит 178 наименований.

Глава 1. Анализ состояния предметной области. Постановка задач исследования

1.1. Анализ нормативно-правовой базы, регламентирующей подходы к оценке угроз компьютерных атак

Методология оценки угроз КА базируется на нормативно-правовой базе Российской Федерации (РФ), в том числе,

- ФЗ «О персональных данных» от 27.07.2006 № 152-ФЗ [1] и Приказе ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [2], регламентирующих защиту персональных данных (ПД) данных;
- приказе ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [3], регламентирующем ЗИ в государственных информационных системах (ГИС);
- ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ № 187 [52], Приказе ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (ред. приказов ФСТЭК России от 9 августа 2018 № 138, от 26 марта 2019 г. № 60, от 20 февраля 2020 г. № 35) [4], регламентирующих ЗИ в объектах критической информационной инфраструктуры (КИИ) и других нормативных документах.

Например, в Приказе ФСТЭК России № 239 статье 19 раздела «Разработка организационных и технических мер по обеспечению безопасности значимого

объекта» рекомендуется при разработке организационных и технических мер по обеспечению безопасности защищаемого вида информации проводить анализ угроз безопасности информации (БИ).

Далее в соответствии с нормативно-правовой базой РФ под понятием «угроза БИ», следуя [5], будем понимать – «совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа» к информации. Результатом такого доступа могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение информации, а также иные неправомерные действия при их обработке информации в информационной системе (ИС). Для уменьшения угроз БИ, характеризующихся вектором угроз (КА), нормативно-правовые документы предусматривают следующие меры ЗИ: базовый набор мер ЗИ, адаптированный базовый набор мер ЗИ, уточнённый адаптированный базовый набор мер ЗИ и дополненный уточнённый адаптированный базовый набор мер ЗИ. При этом каждый из последующих наборов мер ЗИ дополняет предыдущий. Таким образом, можно связать набор мер ЗИ и вектор КА. Рассмотрим детальнее подходы к определению вектора КА (набора мер ЗИ).

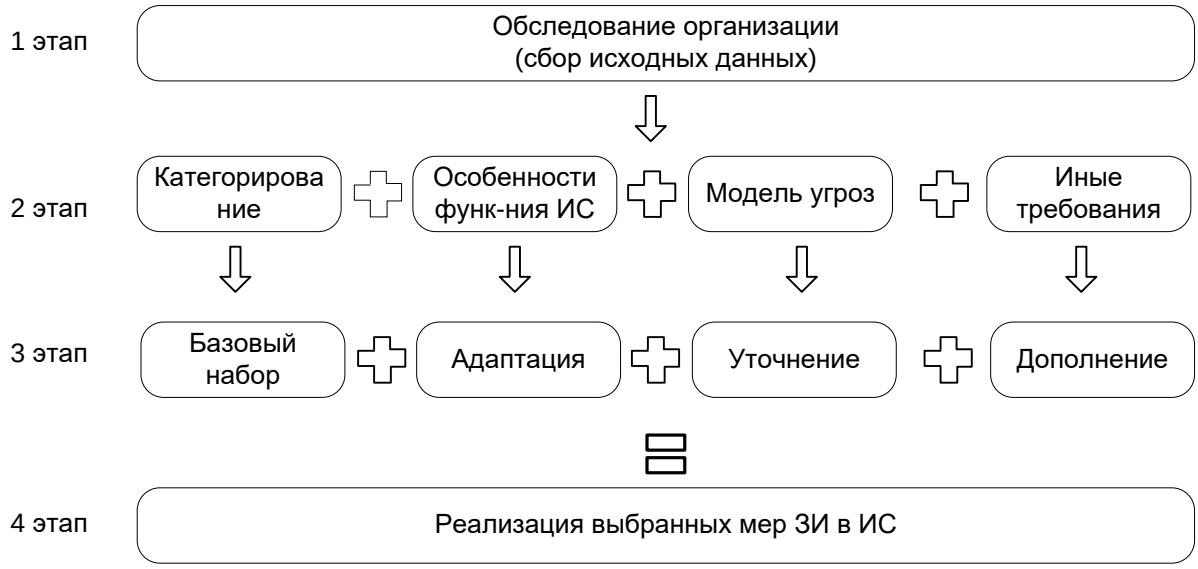

Рисунок 1-1. Структурная схема методики формированию требований при защите ПД, ГИС и объектов КИИ

Для дальнейшего анализа методологии оценки угроз рассмотрим структурную схему методики формирования требований по защите ПД, ГИС и объектов КИИ, разработанную автором на основе требований нормативно-правовых документов [1–5, 52] (Рисунок 1-1).

Из рисунка 1-1 видно, что методика формирования требований по защите ПД, ГИС и объектов КИИ на первом этапе 1 предусматривает обследование ИС организации с целью сбора исходных данных об организации, ИС, телекоммуникационных сетях, типах данных и т.п., в том числе:

- сбор информации о целях создания ИС и задачах, решаемых этой ИС;
- сбор структурно-функциональных характеристик ИС, используемых информационных технологий (ИТ), информации об особенностях функционирования ИС;
- определение информации, подлежащей обработке в ИС и требующей защиты;
- сбор характеристик информации, требующей защиты;
- анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать ИС;
- сбор данных об обладателе информации, операторе и иных уполномоченных лицах;
- сбор сведений об объекте КИИ (наименование объекта, адреса размещения, сфера (область) деятельности, адрес местонахождения, фамилия, имя, отчество и должность руководителя, структурное подразделение, ответственное за обеспечение безопасности значимых объектов, ИНН субъекта и КПП его обособленных подразделений);
- сбор сведений о взаимодействии объекта КИИ и сетей электросвязи (категория сети электросвязи, наименование оператора связи и (или) провайдера хостинга, цель взаимодействия с сетью электросвязи, способ взаимодействия с сетью);

- сбор сведений о программных и программно-аппаратных средствах, используемых на объекте КИИ;
- существующие организационные и технические меры, применяемые для обеспечения безопасности значимого объекта КИИ (организационные меры, технические меры).

Данные полученные на этапе 1 используются на этапах 2 для определения и анализа угроз БИ, на основании которых на этапе 3 методики формируются меры ЗИ, реализуемые далее на этапе 4 (см. Рисунок 1-1).

1.1.1. Определение базового набора мер защиты информации

Основная задача базового набора мер ЗИ, выбираемого на основе анализа результатов категорирования, перечисленных выше объектов организации, состоит в защите от базового вектора КА. Здесь под категорированием мы понимаем определение уровня защищенности (УЗ) ПД [53], класса защищенности (КЗ) [3] и категории значимости [54].

Определение базового набора мер защиты информации ГИС

Методология определения требований по ЗИ, обрабатываемой в ГИС, предусматривает, в первую очередь, отнесение ГИС [3] к одному из трех КЗ, определяющих тип базового набора мер ЗИ [3].

Рассмотрим порядок определения КЗ, зависящего от двух параметров:

$$КЗ = F_{КЗ}\left(УЗН, М\right),$$

где

$УЗН = F_{УЗН}\left(К, Ц, Д\right)$ – уровень значимости информации, определяемый по степени возможного ущерба для обладателя информации и/или оператора от нарушения конфиденциальности (далее – *К*), целостности (далее – *Ц*) или доступности (далее – *Д*) информации;

$М \in \{федеральный; региональный; объектовый\}$ – масштаб ИС.

Значение функции $F_{УЗН}\left(К, Ц, Д\right)$ определяется на основе таблицы 1-1 [3] с помощью метода экспертных оценок:

$$F_{УЗН}(К,Ц,Д)=1, \text{ если } К=1 \vee Ц=1 \vee Д=1; \quad (1.1)$$

$$F_{УЗН}(К,Ц,Д)=2, \text{ если } (К\neq 1 \wedge Ц\neq 1 \wedge Д\neq 1)\wedge(К=2 \vee С=2 \vee Д=2); \quad (1.2)$$

$$F_{УЗН}(К,Ц,Д)=3, \text{ если } К=3 \wedge Ц=3 \wedge Д=3. \quad (1.3)$$

Таблица 1-1. Степени ущерба от КА

Высокая степень ущерба	Средняя степень ущерба	Низкая степень ущерба
1	2	3
возможны существенные негативные последствия в различных областях деятельности и (или) ИС и (или) оператор не могут выполнять возложенные на них функции	возможны умеренные негативные последствия в различных областях деятельности и (или) ИС и (или) оператор не могут выполнять хотя бы одну из возложенных на них функций	возможны незначительные негативные последствия в различных областях деятельности и (или) ИС и (или) оператор могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств

Значение параметра *М* выбирается в зависимости от масштаба ИС:

- ИС, функционирующая на территории РФ (в пределах федерального округа) и имеющая сегменты в субъектах РФ, муниципальных образованиях и (или) организациях, относится к ИС федерального масштаба;
- ИС, функционирующая на территории субъекта РФ и имеющая сегменты в одном или нескольких муниципальных образованиях и (или) подведомственных организациях, относится к ИС регионального масштаба;
- ИС, функционирующая на объектах отдельного федерального органа государственной власти, органа государственной власти субъекта РФ, муниципального образования и/или организации и не имеющая сегментов в иных организациях, относится к ИС объектового масштаба.

КЗ ИС (значение функции $F_{КЗ}(УЗН,М)$) определяется в соответствии с таблицей 1-2 [3]:

$$КЗ = F_{КЗ}(УЗН,М) = КЗ1, \quad (1.4)$$

если

$$УЗН = F_{УЗН}(К, Ц, Д) = 1 \wedge \begin{pmatrix} М = федеральный \vee \\ М = региональный \vee \\ М = объектовый \end{pmatrix},$$

или

$$УЗН = F_{УЗН}(К, Ц, Д) = 2 \wedge М = федеральный;$$

$$КЗ = F_{КЗ}(УЗН, М) = КЗ2, \quad (1.5)$$

если

$$УЗН = F_{УЗН}(К, Ц, Д) = 2 \wedge (М = региональный \vee М = объектовый),$$

или

$$УЗН = F_{УЗН}(К, Ц, Д) = 3 \wedge М = федеральный;$$

$$КЗ = F_{КЗ}(УЗН, М) = КЗ3, \quad (1.6)$$

если

$$УЗН = F_{УЗН}(К, Ц, Д) = 3 \wedge (М = региональный \vee М = объектовый).$$

Таблица 1-2. Класс защищённости ИС

Уровень значимости информации	Масштаб ИС		
	Федеральный	Региональный	Объектовый
*УЗН*1	*КЗ*1	*КЗ*1	*КЗ*1
*УЗН*2	*КЗ*1	*КЗ*2	*КЗ*2
*УЗН*3	*КЗ*2	*КЗ*3	*КЗ*3

Таким образом, алгоритм определения КЗ реализуется выполнением следующей последовательности действий:

1. Определить в соответствие с таблицей 1-1 степень ущерба по свойству БИ «конфиденциальность» (значение переменной *К*).

2. Определить в соответствие с таблицей 1-1 степень ущерба по свойству БИ «целостность» (значение переменной *Ц*).

3. Определить в соответствие с таблицей 1-1 степень ущерба по свойству БИ «целостность» (значение переменной *Д*).

4. Определить масштаб ИС.

5. Определить в соответствие с (1.1)–(1.3) УЗН информации (значение функции $УЗН = F_{УЗН}(К, Ц, Д)$).

6. Определить в соответствие с (1.4)–(1.6) КЗ ИС (значение функции $КЗ = F_{КЗ}(УЗН, М)$).

Таким образом, базовый набор мер ЗИ для ГИС определяется в соответствии с таблицей мер ЗИ соответствующего КЗ [3] основываясь на масштабе ИС и экспертной оценке оператором размера ущерба базовым свойствам информации. При этом нормативно-правовые документы предусматривают использование одного из трех базовых мер ЗИ. В этой связи понятно, что для ГИС следует рассматривать, соответственно, три усредненных наборов векторов актуальных угроз БИ. Это с одной стороны, существенно облегчает подход к определению требований, однако, с другой стороны, для каждой конкретной организации данные требования могут оказаться избыточными и/или недостаточными. При этом использование экспертных оценок для определения КЗ создает риск субъективности и не гарантирует повторяемость результата.

Необходимо отметить, что экспертная оценка ущерба в описанном выше алгоритме осуществляется с точки зрения специалиста ИБ, но не нарушителя. При этом может оказаться, что экспертная оценка КЗ может оказаться недостаточно точной, так как нарушитель, как правило, проводит КА на наименее защищенные компоненты ИС. В этой связи при оценке КЗ ИС и определении перечня мер по ее защите необходимо учитывать наиболее вероятные вектора КА, чего, однако, действующая нормативно-правовая документация не предусматривает.

Определение базового набора мер защиты ИСПД

Методология определения требований по ЗИ, обрабатываемых в ИСПД, в первую очередь зависит от отнесения ИСПД к одному из четырех УЗ ПД, определяющих тип базового набора мер ЗИ [53].

УЗ ПД — это комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности ПД при их обработке в ИСПД. УЗ определяется на основании типа угроз, связанных с не декларированными возможностями, категорией ПД, количества и типов субъектов в ИСПД [53].

Рассмотрим порядок определения УЗ.

$$УЗ = F_{УЗ}\left(K_{ПД}, C, C_M, T_y\right),$$

где

$K_{ПД} \in \{общедоступные; биометрические; специальные; иные\}$ – категория ПД, обрабатываемых в ИСПД;

$C \in \{собственные\ сотрудники; иные\ субъекты\}$ – тип субъектов ПД, чьи данные обрабатываются в ИСПД;

C_M – максимальное количество субъектов ПД, не относящихся к собственным сотрудникам организации, ПД которых обрабатывается в ИСПД;

$T_y \in \{1;2;3\}$ – тип актуальных угроз.

Значение $K_{ПД}$ определяют на основе таблицы 1-3 в зависимости от обрабатываемых сведениях о субъекте ПД [53].

Таблица 1-3. Категория ПД

Категория ПД	Описание категории ПД
Общедоступная	сведения о субъекте ПД, полный и неограниченный доступ к которым предоставлен самим субъектом
Биометрическая	данные, характеризующие биологические или физиологические особенности субъекта ПД, например, отпечатки пальцев
Специальная	информация о национальной и расовой принадлежности субъекта ПД, о религиозных, философских либо политических убеждениях, информацию о здоровье и интимной жизни субъекта ПД
Иная	сведения о субъекте ПД, не представленные в трех других категориях

Тип актуальных угроз T_y определяется экспертным путем из трех вариантов в соответствии с таблицей 1-4 [53].

Таблица 1-4. Тип актуальных угроз

Тип актуальных угроз	Наличием не декларированных (недокументированных) возможностей в системном программном обеспечении (ПО), используемом в ИСПД	Наличием не декларированных возможностей в прикладном ПО, используемом в ИСПД
1	+	–
2	–	+
3	+	+

Ниже приведен подход к определению УЗ.

$$УЗ = F_{УЗ}\left(K_{ПД}, C, C_M, T_y\right) = 1УЗ, \quad (1.7)$$

если

$$(К_{ПД} = специальные \vee К_{ПД} = биометрические) \wedge Т_{у} = 1,$$

или

$$К_{ПД} = специальные \wedge Т_{у} = 2 \wedge С = иные\ субъекты \wedge (С_{М} > 100тыс.),$$

или

$$К_{ПД} = иные \wedge Т_{у} = 1 \wedge С = иные\ субъекты \wedge (С_{М} > 100тыс.);$$

$$УЗ = F_{УЗ}\left(К_{ПД}, С, С_{М}, Т_{у}\right) = 2УЗ, \quad (1.8)$$

если

$$К_{ПД} = общедоступные \wedge (Т_{у} = 1 \vee (Т_{у} = 2 \wedge С = иные\ субъекты \wedge (С_{М} > 100тыс.))),$$

или

$$К_{ПД} = иные \wedge Т_{у} = 2 \wedge С = иные\ субъекты \wedge (С_{М} > 100тыс.),$$

или

$$К_{ПД} = иные \wedge Т_{у} = 1 \wedge (С = собственные\ сотрудники \vee$$
$$(С = иные\ субъекты \wedge С_{М} < 100тыс.),$$

или

$$К_{ПД} = биометрические \wedge Т_{у} = 2,$$

или

$$К_{ПД} = специальные \wedge Т_{у} = 2 \wedge (С = собственные\ сотрудники \vee$$
$$(С = иные\ субъекты \wedge С_{М} < 100тыс.),$$

или

$$К_{ПД} = специальные \wedge Т_{у} = 3 \wedge С = иные\ субъекты \wedge (С_{М} > 100тыс.);$$

$$УЗ = F_{УЗ}\left(К_{ПД}, С, С_{М}, Т_{у}\right) = 3УЗ, \quad (1.9)$$

если

$$((К_{ПД} = специальные \wedge Т_{у} = 3) \vee ((К_{ПД} = иные \vee К_{ПД} = общедоступные) \wedge Т_{у} = 2)$$
$$\wedge (С = собственные\ сотрудники \vee (С = иные\ субъекты \wedge С_{М} < 100тыс.),$$

или

$$К_{ПД} = биометрические \wedge T_y = 3,$$

или

$$К_{ПД} = иные \wedge T_y = 3 \wedge C = иные\ субъекты \wedge (C_M > 100тыс.);$$

$$УЗ = F_{УЗ}\left(К_{ПД}, C, C_M, T_y\right) = 4УЗ, \quad (1.10)$$

если

$$К_{ПД} = общедоступные \wedge T_y = 3,$$

$$К_{ПД} = иные \wedge T_y = 3 \wedge (C = собственные\ сотрудники \vee$$
$$(C = иные\ субъекты \wedge C_M < 100тыс.).$$

Данный подход представлен в виде таблицы 1-5.

Таблица 1-5. УЗ ИСПД

Категории ПД		Специальные			Биометрические	Иные			Общедоступные		
Собственные работники		Нет	Нет	Да	Не важно	Нет	Нет	Да	Нет	Нет	Да
Количество субъектов		>100 тыс.	<100 тыс.	Любое	Любое	>100 тыс.	<100 тыс.	Любое	>100 тыс.	<100 тыс.	Любое
Тип актуальных угроз	1	1УЗ	1УЗ	1УЗ	1УЗ	1УЗ	2УЗ	2УЗ	2УЗ	2УЗ	2УЗ
	2	1УЗ	2УЗ	2УЗ	2УЗ	2УЗ	3УЗ	3УЗ	2УЗ	3УЗ	3УЗ
	3	2УЗ	3УЗ	3УЗ	3УЗ	3УЗ	4УЗ	4УЗ	4УЗ	4УЗ	4УЗ

Таким образом, алгоритм определения УЗ реализуется выполнением следующей последовательности действий:

1. Определить в соответствие с таблицей 1-3 категорию ПД (значение переменной $К_{ПД}$).

2. Определить тип субъектов ПД, чьи данные обрабатываются в ИСПД.

3. Определить максимальное количество субъектов ПД, не относящихся к собственным сотрудникам организации, ПД которых обрабатывается в ИСПД.

4. Определить в соответствии с таблицей 1-4 тип актуальных угроз.

5. Определить в соответствие с (1.7)–(1.10) УЗ ИСПД (значение функции $УЗ = F_{УЗ}\left(К_{ПД}, C, C_M, T_y\right)$).

Базовый набор мер ЗИ для ИСПД представляет собой жестко определяемый набор требований к реализации системы ИБ в зависимости от четырех типов УЗ [2]. Это приводит к тому, что при проектировании системы ИБ используется

статическая матрица усредненных требований, которая базируется на 4 усредненных векторах КА. Для каждой конкретной организации данные требования могут оказаться избыточными или недостаточными, что с одной стороны, приводит к недостаточной защищенности и потерям организации из-за КА, а с другой стороны к не эффективному расходованию ресурсов организации (как финансовых, так и человеческих), так как для предприятий малого или среднего бизнеса объем требований может быть избыточным.

Определение базового набора мер защиты КИИ

Базовый набор мер ЗИ КИИ формируется, исходя из КЗ объекта КИИ. Чтобы выяснить, какие системы являются объектами КИИ, производится категорирование объектов КИИ.

В отличие от вышеописанных методов определения УЗ и КЗ при категорировании объектов КИИ определены эксперты, а именно, состав комиссии по категорированию, в которую необходимо включить:

- генерального директора или уполномоченное им лицо;
- специалистов производства;
- специалистов промышленной безопасности;
- специалистов отдела автоматизированных систем управления технологическим процессом (АСУ ТП);
- специалистов отдела ИТ;
- ответственных за обеспечения безопасности в АСУ ТП;
- работников подразделения по защите государственной тайны;
- специалистов по промышленной безопасности, по гражданской обороне и защите от чрезвычайных ситуаций.

Присвоение категории значимости объекта КИИ проводится экспертами в соответствие с таблицей, приведенной в приложении А, и определяется по формуле:

$$K = \max\left(\max\left(index_j\right)\right), \tag{1.11}$$

где

$index_j \in \{0;1;2;3\}$ – множество возможных экспертных оценок j-го показателя ($index_j = 0$ – незначимый объект КИИ, $index_j = 3$ – объект КИИ 3-ей категории значимости), $j = \overline{1,14}$ – номер показателя. Таким образом, алгоритм категорирования объектов КИИ реализуется выполнением следующей последовательности действий.

1. Определить относится ли организация к субъектам КИИ. Согласно [52] организация является субъектом КИИ, если $ОКВЭД_{организации} \in Сфера_{КИИ}$, где

$$Сфера_{КИИ} \in \left\{ \begin{array}{l} здравоохранение;\ наука;\ транспорт;\ связь;\ энергетика; \\ банковская\ сфера\ и\ иные\ сферы\ финансового\ рынка; \\ топливно-энергетический\ комплекс;\ атомная\ энергии; \\ оборонная;\ ракетно-космическая;\ горнодобывающая; \\ металлургическая;\ химическая\ промышленность. \end{array} \right\}$$

Если $ОКВЭД_{организации} \notin Сфера_{КИИ}$, то выполнение требований по ЗИ КИИ не требуется, однако, может привести к организационным коллизиям. Например, организации, осуществляющие деятельность в сфере жилищно-коммунального хозяйства, не относятся к субъектам КИИ, однако, результатом реализации КА на данные организации может стать прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов водоснабжения и канализации (один из показателей категорирования объектов КИИ) [54].

2. Определить критические процессы в организации. (Экспертным путем, комиссией по категорированию из списка всех процессов организации выделяются процессы, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка [54]).

3. Определить объекты КИИ, связанные с критичными процессами.

4. Провести категорирование объектов КИИ в соответствии с (1.7) путем присвоения категории значимости.

В зависимости от категории значимости в [54] определен базовый набор мер ЗИ, которые основаны на использовании широкого перечня показателей, применяемых для оценки ущерба. Однако экспертный подход к оценке категории значимости объекта КИИ не гарантирует повторяемости результатов при использовании, описанной выше, методики, а потому имеет место известная субъективность оценки категории значимости объектов КИИ однотипных объектов. При этом необходимо отметить, что использование только 3-х базовых наборов мер ЗИ возникает необходимость анализа статической матрицы усредненных требований, составленной из 3-х усредненных векторов КА.

1.1.2. Адаптация базового набора мер защиты информации

На данном этапе (при наличии соответствующих возможностей) на основе анализа структурно-функциональных характеристик ИС, ИТ и особенностей их функционирования сокращают число требований за счет исключения из базового вектора КА некоторых возможных КА. Например, если в организации отсутствуют ИТ, для которых определены меры в базовом наборе мер ЗИ, в соответствие с [4] из вектора КА можно исключить часть КА, включенных в базовый набор мер ЗИ, определенного на основе КЗ. Например, если в организации не используют технологии виртуализации, то вероятность КА на них тождественно равняется 0, поэтому, меры ЗИ, связанные с технологиями виртуализации, из базового набора исключаются, соответственно, изменяется и вектор КА.

1.1.3. Уточнение адаптированного базового набора мер защиты информации

Уточнение адаптированного базового набора мер ЗИ реализуется путем формирования МУ. Фактически анализ угроз БИ влияет только на дополнение требований к реализации систем ИБ, определенных законодательством РФ.

РОассмотрим более подробно методологию формирования МУ [5-8]. Целью определения угроз БИ является установление возможности нарушения свойств

информации, содержащейся в ИС, автоматизированных системах управления, информационно-телекоммуникационных сетях, информационно-телекоммуникационных инфраструктурах центров обработки данных и облачных инфраструктурах (далее системы и сети) и приведет ли нарушение к наступлению негативных последствий (ущербу) для обладателя информации. В 2021 г. ФСТЭК России утверждена «Методика определения угроз БИ» [5] (далее Методика ФСТЭК России), предусматривающая моделирование угроз со стороны нарушителя (антропогенные угрозы).

Формирование модели угроз в соответствии с Методикой ФСТЭК России

При составлении МУ необходимо [5]:

1. Определить возможные объекты воздействия, путем инвентаризации систем и сетей.

2. Определить источники угроз БИ.

3. Оценить возможности нарушителей по реализации угроз БИ:

– способы реализации угроз БИ;

– сценарии реализации угроз БИ в системах и сетях;

– возможности реализации угроз БИ.

4. Определить негативные последствия от реализации (возникновения) угроз БИ.

В методологии оценки угроз, априори полагается, что каждая из угроз формируется взаимосвязью источников угроз, способов реализации угроз, уязвимостей и последствий [5]. Обобщённая схема канала реализации угроз БИ представлена на рисунке 1-2.

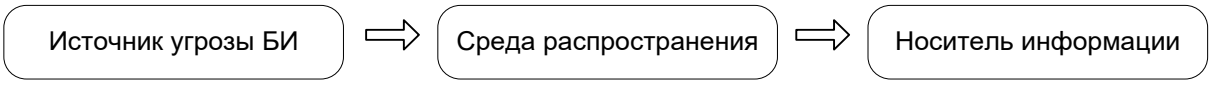

Рисунок 1-2. Структурная схема канала реализации угрозы

Под источником угрозы в методологии ФСТЭК России [5] понимается нарушитель – физическое лицо (группа лиц), осуществляющие преднамеренную или непреднамеренную реализацию угроз БИ путем несанкционированного

доступа и (или) воздействия на информационные ресурсы и (или) компоненты систем и сетей.

Угроза БИ в ИС и компьютерных сетях (КС) представляется кортежем:

$$УБИ_j = \{нарушитель; уязвимость; способ\ реализации;$$
$$объект\ воздействия;\ последствия\ от\ реализации\ угрозы\}.$$

В соответствии с нормативными документами ФСТЭК России классификация нарушителей проводится как с точки зрения наличия права доступа в контролируемую зону к ИС и КС (при этом выделяют: внешнего нарушителя (тип I) и внутреннего нарушителя (тип II)), так и с точки зрения навыков нарушителя. Выделяют следующие типы навыков нарушителя:

- базовые возможности по реализации угроз БИ (*H1*);
- базовые повышенные возможности по реализации угроз БИ (*H2*);
- средние возможности по реализации угроз БИ (*H3*);
- высокие возможности по реализации угроз БИ (*H4*).

Детальное описание классификации нарушителей приведено в приложении В. (Напомним, что с точки зрения документов ФСБ России нарушитель может действовать на различных этапах жизненного цикла криптографического средства и среды его функционирования [8]). Для создания модели нарушителя необходимо:

1. Определить этапы жизненного цикла криптографического средства, на которых может воздействовать нарушитель.

2. Составить модель нарушителя, выявив возможные типы нарушителей и учтя при этом, что:

- нарушитель H_{i+1}, совершающий КА после нарушителя H_i, здесь $1 \le i \le 5$, может использовать уязвимости и средства КА, использованные ранее нарушителем H_i,
- если внешний нарушитель обладает возможностями, аналогичными возможностям нарушителя типа H_i, он также обозначается как нарушитель типа H_i, при этом $2 \le i \le 6$;

- составить перечень лиц, которые не рассматриваются в качестве нарушителей;
- выдвинуть предположение о невозможности либо о возможности и характере сговора нарушителей.

3. Сделать предположение об информации об объектах КА, имеющейся у нарушителя.

4. Сделать предположение о средствах КА, имеющихся у нарушителя.

5. Описать каналы КА.

6. Определить тип нарушителя:

- нарушитель относится к типу H_i, если среди его предполагаемых возможностей нет тех, которые уникальны для нарушителей типа H_j, $j > 1$;
- при отнесении нарушителя к типу H_6 необходимо согласовать модель нарушителя с ФСБ России.

Тип нарушителя определяется экспертным методом.

При формировании перечня угроз БИ систем и сетей [5] и объектов КИИ [4] необходимо использовать банк данных угроз ФСТЭК России (более 200 угроз) [6] и учитывать угрозы, отраслевых МУ, описание векторов КА, содержащихся в общедоступных базах данных (*CAPEC, ATT&CK, OWASP, STIX, WASC* и др.)

При защите ПД банк данных угроз ФСТЭК России [6] может быть дополнен, с помощью [1]:

- актуальных угроз для различных сфер деятельности, сформированных органами государственной власти субъектов РФ, Банк России, органы государственных внебюджетных фондов и т.п.;
- перечня дополнительных угроз, определенных оператором и/или объединением операторов ПД;
- документации на системы и сети;
- описания критических для организации процессов.

В соответствии с вышеизложенным для проведения анализа всего перечня угроз БИ необходимо как минимум описать 27200 уже определенных угроз. Оценка угроз БИ проводится группой экспертов, состоящей из не менее чем трех человек, в которую могут входить:

- специалисты ИБ;
- специалисты, ответственные за эксплуатацию систем и сетей;
- специалисты основных (профильных) подразделений обладателя информации.

Для сокращения объема оцениваемых угроз определен алгоритм оценки актуальности. В соответствии с которым необходимо ограничить перечень рассматриваемых объектов, только теми, воздействие на которые повлечет к негативным последствиям ($НП_j$):

- нарушению прав граждан;
- возникновению ущерба в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности государства;
- возникновению финансовых, производственных, репутационных или иных рисков (видов ущерба) для обладателя информации, оператора.

Идентифицированная экспертным путем угроза БИ подлежит нейтрализации (блокированию), если она является актуальной $УБИ_j = A$ для систем и сетей:

$$УБИ_j = F_{УБИ}(НП_j, СРУ_j) \quad (1.12)$$

где

$НП_j = \{низкий; средний; высокий\}$ — величина, характеризующая негативные последствия для объекта, определяется экспертным путем;

$СРУ_j = \{да; нет\}$ — наличие способа реализации угрозы БИ, определяется экспертным путем.

Перечень способов реализации угроз БИ ($СРУ_j$) выбирается экспертами из следующего списка (которым, однако не ограничивается):

1. Использование уязвимостей (уязвимостей кода ПО, уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей).

2. Внедрение вредоносного программного обеспечения (ВПО) [7].

3. Использование недекларированных возможностей ПО и/или программно-аппаратных средств.

4. Установка программных и (или) программно-аппаратных закладок в ПО и (или) программно-аппаратные средства.

5. Формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных.

6. Перехват (измерение) побочных электромагнитных излучений и наводок (других физических полей) для доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации.

7. Инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации.

8. Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию).

9. Ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств.

Традиционно, в экспертном методе принятия решений используется некоторая функция, зависящая от экспертных оценок, которую в нашем исследовании будем обозначать $F_{УБИ}$. При этом экспертные оценки получают «опросным методом с составлением анкеты, в которой указываются вопросы и возможные варианты ответа в единой принятой шкале измерений («низкий», «средний», «высокий» или «да», «нет» или иные шкалы). В этой связи вопросы,

задаваемые экспертам, должны быть четкими и однозначно трактуемыми, предполагать однозначные ответы» [5]. Экспертный метод оценки имеет следующие этапы [5]:

- каждый эксперт проводит оценку оцениваемого параметра (рекомендуется не мене двух раундов оценки);
- результаты оценки заносятся в таблицу;
- после оценки каждым из экспертов отбрасываются минимальные и максимальные значения;
- определяется среднее значение оцениваемого параметра в каждом раунде;
- определяется итоговое среднее значение оцениваемого параметра.

Таким образом, алгоритм определения актуальных угроз БИ реализуется выполнением следующей последовательности действий.

1. Определение негативных последствий:

- анализ документации систем и сетей и иных исходных данных;
- экспертная оценка негативных последствий.

2. Определение объектов воздействия:

- анализ документации систем и сетей и иных исходных данных;
- инвентаризация систем и сетей;
- определение группы информационных ресурсов и компонентов систем и сетей.

3. Оценка возможности реализации угроз и их актуальность:

- определение источников угроз БИ (экспертная оценка);
- оценка способов реализации угроз БИ (экспертная оценка);
- оценка актуальности угроз БИ (экспертная оценка).

Таким образом, при анализе угроз БИ учитывается уровень доступа нарушителя к системам и сетям и его возможности, представленные в виде ограниченного набора вариантов в методических документах ФСТЭК России и ФСБ России. Методология анализа предусматривает оценку угроз БИ с точки зрения организации/оператора/владельца информации, в то время как

нарушитель, выбирая объект КА, зачастую не владеет этой информацией, а значит, выбор объекта и способов КА производит на основании иных данных.

При этом актуальность угрозы определяется экспертным путем. Требования к компетенции привлекаемых экспертов для оценки угроз в последней методологии ФСТЭК России были введены [5] и в описании «Квалификационных характеристик должностей» [55]. К требованиям к квалификации/компетенции эксперта, выполняющим анализ угроз БИ – экспертам ИБ отнесены:

1. Наличие базового высшего образования в области ИБ. В частности, должностные обязанности, связанные с определением, оценкой и переоценкой угроз ИБ, определением уязвимостей ПО и аппаратного обеспечения, может выполнять сотрудник не ниже специалиста ИБ в ключевых системах информационной инфраструктуры.

2. Наличие опыты работы в области ИБ.

3. Владение агрегированной информацией о законодательстве в области ИБ, средствах и методах ЗИ, о возможных угрозах БИ, уязвимостях, технологиях обнаружения вторжения, оценке рисков ИБ.

4. Умение обеспечить необходимый уровень ИБ организации путем эффективного использования агрегированной информации.

При этом в методических документах ФСТЭК России обозначены риски использования экспертного метода [5]. А именно, независимо от результата формирования экспертной группы при оценке угроз БИ существуют субъективные факторы, связанные с психологией принятия решений. Возможные риски:

- занижение или завышение экспертами прогнозов при оценке угроз БИ;
- пропуску отдельных угроз БИ;
- неоправданные затраты на нейтрализацию неактуальных угроз.

При этом, априори, понятно, что привлечь на практике трех независимых экспертов ИБ с одинаковым уровнем компетенций весьма проблематично.

С другой стороны, фактически анализ угроз БИ влияет только на дополнение требований к реализации систем ИБ, определенных

законодательством РФ. В соответствии с требованиями [4], дополнение адаптированного базового набора мер ЗИ возможно в соответствии с дополнительными угрозами и происходит только из строго определенного набора мер.

1.1.4. Дополнение уточнённого адаптированного базового набора мер защиты информации

Из вышеизложенного следует, что рекомендуемый подходе к формированию набора мер ЗИ для ПД, ГИС и объектов КИИ предполагает использование и других руководящих документов ФСТЭК и ФСБ России. В этой связи, если организация одновременно подпадает под объект КИИ, обрабатывает ПД и имеет ГИС, при проектировании системы ИБ необходимо учитывать требования всех упомянутых нормативных документов. Например, для значимых объектов КИИ, являющихся ИСПД, необходимо учитывать Требования к защите ПД при их обработке в ИСПД (постановление Правительства РФ от 01.11.2012 г. № 1119).

1.1.5. Существующие ограничения Методики ФСТЭК России

На практике реализовать Методику ФСТЭК России одним экспертом ИБ (и даже группой из трех экспертов ИБ) оказывается весьма затруднительным, так как нормативно-правовая база РФ предъявляет жесткие требования к реализации системы ИБ в зависимости либо от уровня градации типа ИС, а именно, класса защищаемых ИС [3], либо от уровня защищенности [2], либо от категории значимости [4]. В законодательстве РФ предусмотрено не более 4 типов ИС. Как следствие, при проектировании системы ИБ используется статическая матрица усредненных требований, которая базируется на усредненной модели угроз и модели нарушителя. Для каждой конкретной организации данные требования могут оказаться избыточными или недостаточными, что с одной стороны, приводит к недостаточной защищенности и потерям организации из-за КА, а с

другой стороны к неэффективному расходованию ресурсов организации (как финансовых, так и человеческих).

Фактически анализ угроз БИ влияет только на дополнение требований к реализации систем ИБ, определенных законодательством РФ. Так в соответствии с [4] исключить требование из базового набора мер по обеспечению ИБ, определенного на основе категории значимости, возможно только, если в организации отсутствуют ИТ, для которых определены меры в базовом наборе. Дополнения требований в соответствии с дополнительными угрозами также выбирают из строго определенного набора мер.

Статистический подход к проектированию не позволяет выявить и спрогнозировать новые вектора КА и их динамические изменения.

Ключевые ограничения классической методологии обусловлены следующими причинами:

- перечень угроз БИ формируется только для объектов, воздействие КА на которые приводит к негативным последствиям [5];
- применение экспертных оценок создает риск субъективности и не гарантирует повторяемость результата;
- анализ угроз БИ формируется с точки зрения владельца информации;
- система ЗИ строится на базе статической матрицы усредненных требований, имеющей относительно небольшое количество градаций/вариаций (не более 4);
- при построении модели угроз, модели нарушителя и системы ЗИ рассматривается определенное временное сечение (дата построения). Отсутствуют методологии, обеспечивающие учет динамики изменения векторов КА и их прогнозирование.

Таким образом, существующий подход к проектированию системы ИБ не позволяет выявить и спрогнозировать новые вектора КА и предсказать их динамические изменения.

1.2. Анализ международных методик, используемых для оценки угроз компьютерных атак

Анализ международных нормативных документов в области ИБ [9–17] позволяет сделать вывод о том, что международные подходы различны по реализации. Рассмотрим две наиболее известных методологии: методология *IT-Grundschutz* по построению системы управления информационной безопасности (СУИБ) для ИБ информационных структур с помощью стандартных мер ЗИ [9–12] и методологию *ISO 2700x* по построению СУИБ и оценки рисков ИБ [13-17]. Остальные международные методологии являются синергией методологий *IT-Grundschutz* и *ISO 2700x.*

1.2.1. Методология *IT-Grundschutz*

Структурная схема методики формирования мер ЗИ на базе серии стандартов *BSI-Standard 100-x* [9–12] приведена на рисунке 1-3.

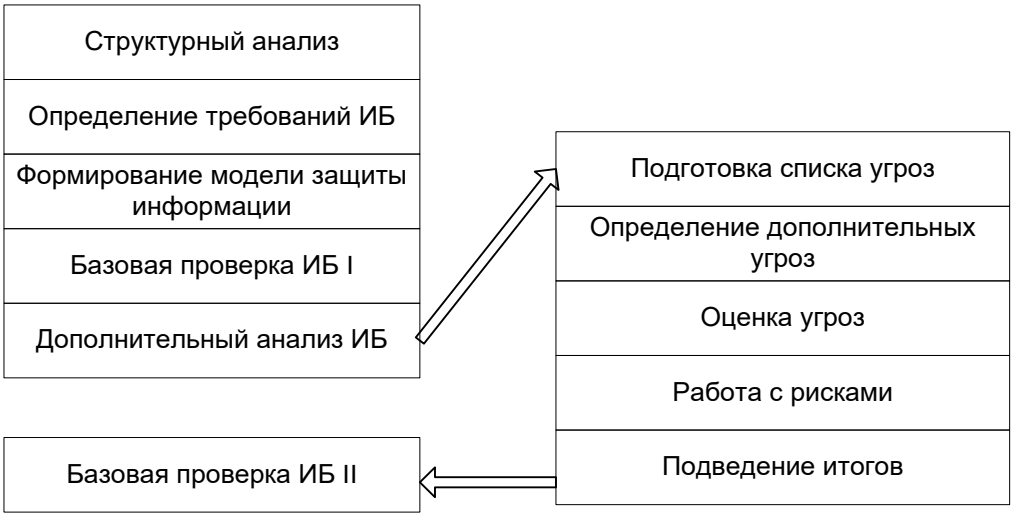

Рисунок 1-3. Структурная схема методики формирование мер ЗИ на базе серии стандартов *BSI-Standard 100-x*

Анализ рисков и формирование требований к ЗИ в соответствии с методологией создания СУИБ, разработанной немецким федеральным ведомством по ИБ (*BSI*) «*IT-Grundschutz*» производится в несколько этапов (см. рисунок 1-3). Подход, используемый в данной методологии, близок к подходу,

предусмотренному нормативными документами РФ, описанным в разделе 1.1. Рассмотрим более подробно этапы методологии *IT-Grundschutz*.

Структурный анализ

Структурный анализ – этап предварительного сбора информации о системе, цель которого состоит в определении объектов (активов), подлежащих защите. Структурный анализ декомпозируется на следующие подзадачи (см. Рисунок 1-4):

1. Подготовка плана сети. (План сети – это графическое представление компонентов, используемых в рассматриваемых ИТ – и коммуникационных технологиях, а также способа их объединения в сеть. План сети должен включать в себя все уровни модели *OSI*).

2. Сбор информации о компонентах ИС. (Здесь составляется список компонентов, существующих и планируемых ИС, в форме таблицы. При этом основное внимание уделяется технической реализации ИС. На данном этапе компоненты ИС рассматриваются целиком (например, сервер *UNIX*), но не их отдельные элементы, например, компьютер, клавиатуру, дисплей и т. д.).

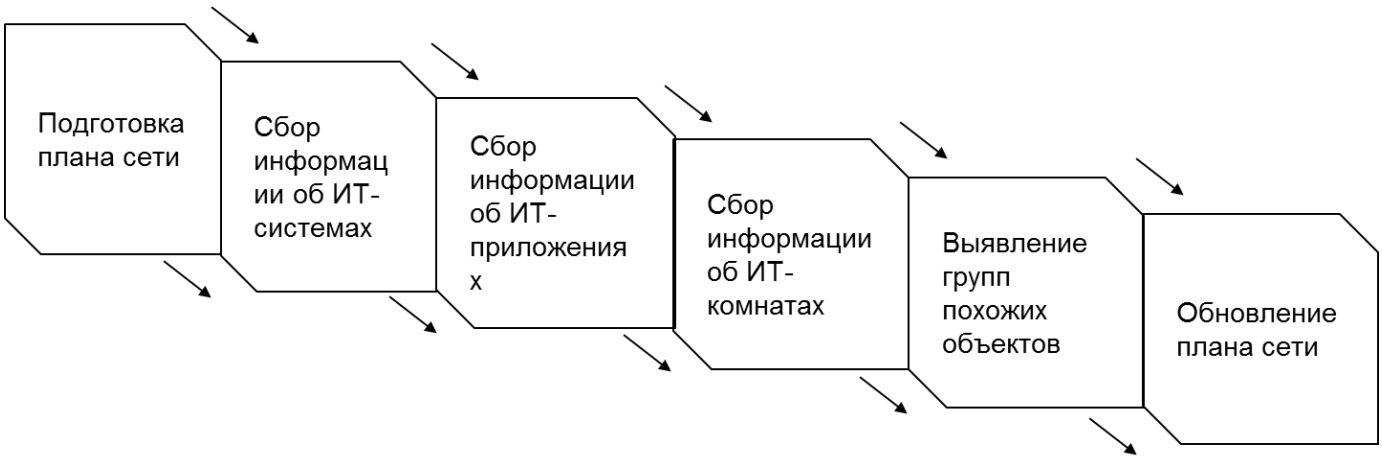

Рисунок 1-4. Подзадачи структурного анализа

3. Сбор информации о приложениях ИС. (Подготавливается информация о приложениях, запущенных или планируемые к запуску в рассматриваемых ИС. Результатом является сводка сведений о том какое основное ПО используется и/или в каких ИС. При этом фиксируются взаимосвязи между приложениями (например, зависимость приложения от конкретной базы данных). Также

собирается информация о тех приложениях, для которых не должно быть нарушено хотя бы одно из 3-х известных свойств обрабатываемой в них информации – конфиденциальность, целостность, доступность $(К, Ц, Д)$. Таким образом, меры ЗИ применяются к объектам (активам), ценным с точки зрения владельца информации/актива.

4. Сбор информации о помещениях ИС. (Составляется список всех зданий и помещений, в которых расположены компоненты ИС, в том числе технические помещения, например, серверные, архивы носителей данных. Если компоненты ИС размещены в стойке, а не в специальном техническом помещении, шкаф должен быть записан как помещение. В список включаются помещения, в которых хранится информация, требующая защиты или обрабатываемая иным образом).

5. Идентификация групп схожих объектов (активов).

Выявление групп похожих объектов (активов) способствует снижению сложности модели, защищаемой ИС. Компоненты ИС относят укрупненной группе, если все компоненты:

- однотипны;
- имеют идентичные или почти идентичные конфигурации;
- подключены к сети одинаковым или почти одинаковым образом (например, на одном коммутаторе);
- подчиняются одинаковым административным и инфраструктурным базовым условиям;
- используют одни и те же приложения;
- имеют одинаковые требования к защите.

Группировку рекомендуется проводить по модулям (см. Рисунок 1-5). Модуль – раздел каталогов *IT-Grundschutz*, служащий для структурирования рекомендаций, представленных в этих каталогах, и отражающий отдельные компоненты информационной структуры, использующиеся в различных областях.

После группировки необходимо скорректировать план сети, в котором каждая группа отображается отдельным объектом.

Определение требований ИБ

Цель этапа – определение базового уровня ЗИ, который является адекватным для бизнес-процессов, обрабатываемой информации и используемых ИТ в организации, с точки зрения $К, Ц, Д$.

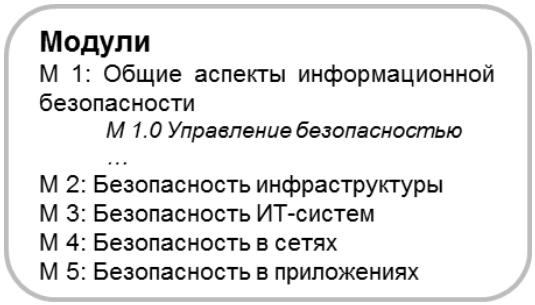

Рисунок 1-5. Модули по методологии *IT-Grundschutz*

Алгоритм определения базового уровня ЗИ реализуется выполнением следующей последовательности действий:

1. Определение категорий требований ИБ, представленных в таблице 1-6.
2. Определение требований ИБ для приложений, ИС, помещений и линий связи.

Таблица 1-6. Категории требований ИБ по методологии *IT-Grundschutz*

Категории требований ИБ	Величина ущерба, который понесет организация
«Стандартная»	Ущерб ограничен
«Высокая»	Ущерб значителен
«Очень высокая»	Ущерб катастрофичен (угроза дальнейшему существованию организации)

В *IT-Grundschutz* для определения категории требований ИБ в зависимости от ущерба, который может угроза БИ для организации, по схеме, приведённой на рисунке 1-6, используют экспертные оценки. При оценке ущерба должен быть привлечен владелец актива, например, ответственный за данное приложение и пользователи приложения.

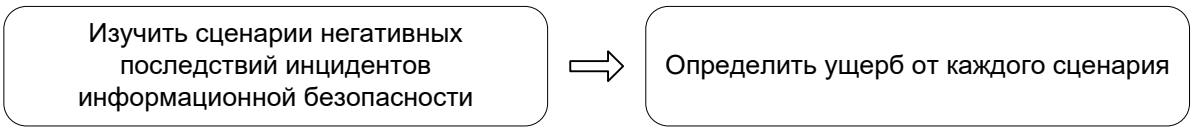

Рисунок 1-6. Порядок определения категорий требований безопасности

Стандартом *BSI* [10] предусмотрены шесть сценариев негативных последствий инцидентов ИБ, представленных в приложении С. При необходимости организация может адаптировать сценарии под свои индивидуальные условия. Набор базовых мер ЗИ в *IT-Grundschutz* имеет ограниченный набор градаций требований, который может быть адаптирован путем изменения (доработки) сценариев негативных последствий.

Определение категорий требований ИБ для приложений, ИС, помещений и линий связи осуществляется последовательно (начиная с приложений и заканчивая помещениями). Для упрощения определения возможного ущерба и его последствий в приложении к стандарту *BSI 100-2* [10] представлен набор вопросов, ответы на которые позволят определить категории требований ИБ для приложений с точки зрения нарушения свойств информации $(К, Ц, Д)$. Требования ИБ рекомендуется рассматривать с общей точки зрения бизнес-процессов или специализированных задач. Преимуществом такого подхода является привлечение руководства организации в качестве регулятора требований ИБ для отдельных приложений.

Для определения требований ИБ ИТ-системы, необходимо рассмотреть потенциальный ущерб для связанных с ней ИТ-приложений. Повреждение или полное повреждение с наиболее серьезными последствиями определяет требования ИБ ИТ-системы (принцип максимума). Требования ИБ помещений вытекают из требований к защите ИТ-систем, установленных в соответствующем помещении, информации, которую они обрабатывают, или носителей информации, хранящихся там (учитывать зависимости, принцип максимума). Требования ИБ к сетевой инфраструктуре определяются на основе требований ИБ, рассматриваемых ИТ-систем, на основе плана сети для проверяемых ИТ-активов, определенного структурном анализе. Если требования ИБ объекта

информационной структуры определены как «стандартные», достаточно внедрить стандартные меры ЗИ из *IT-Grundschutz*. Запланировать дополнительный анализ безопасности необходимо для всех объектов с повышенными требованиями к безопасности.

Формирование модели ЗИ

Цель данного этапа –выбор и адаптация мер ЗИ. Модель ЗИ формируются при помощи модулей *IT-Grundschutz*, которые содержат типовые сценарии угроз и рекомендуемые меры ЗИ для различных компонентов, процедур и ИТ-систем.

Каждый сценарий угрозы БИ является частью упрощенного анализа рисков для типичных областей обработки информации и формирует основу для конкретного пакета мер ЗИ, разработанного *BSI*.

Для соотнесения наборов объектов с модулями стандарта рекомендуется использовать следующие уровни:

1. Общие аспекты ИБ, отнесенные ко всей основной информации или к ее большей части, и включают в себя такие модули, как управление ИБ, организация, персонал, политика резервного копирования данных, концепция защиты от вирусов и т.д.

2. Безопасность инфраструктуры, отнесенная к архитектурным и структурным объектам, таким как здания, помещения, серверная комната, удаленное рабочее место и т.д.

3. ИБ ИС, отнесенная к отдельным компонентам ИТ-систем, таких как серверы, клиенты, автономные системы и т.д.

4. Сетевые аспекты ИБ, отнесенные к аспектам безопасности сетевых соединений и коммуникации систем, не связанных с конкретными ИТ-системами, таким как гетерогенные сети, *WLAN*, модули удаленного доступа и т.д.

5. ИБ приложений, отнесенная к конкретным приложениям, используемым на информационных объектах (электронная почта, веб-сервер, факс-сервер, базы данных и т.д).

Таким образом, в процессе соотношения целевых объектов с модулями создается модель, используя которую, далее этим объектам назначаются типовые

угрозы и соответствующие стандартные меры ЗИ, призванные устранить основные риски.

На этом этапе также необходимо отметить все объекты, задокументированные при структурном анализе, которые не могут быть смоделированы должным образом с помощью модулей, предложенных в каталогах *BSI*, и требующие дополнительного анализа безопасности.

Базовая проверка ИБ

Цель данного этапа состоит в оценке адекватности использованных стандартных мер ЗИ на основе сравнения целевого состояния ИС с ее фактическим состоянием.

Для проведения целевого сравнения ИБ необходимо.

- проверить внутреннюю документацию, которая отвечает за процессы ИБ (рабочие инструкции, руководства и «неформальные» процедуры), оценить степень внедрения стандартов ИБ в организации;
- сформировать перечень сотрудников и сторонних специалистов, взаимодействующих с объектом оценки, для дальнейшего собеседования на предмет реализации внутренней документации.

В рамках проведения сравнения целевого и фактического состояний ИБ ответственные за использование объектов модуля сотрудники опрашиваются на предмет статуса внедрения той или иной меры ЗИ для исследуемого объекта, согласно соответствующему модулю каталогов *IT-Grundschutz*. Происходит сравнение целевых и фактических данных, что описывает текущую степень реализации мер ЗИ.

Степень внедрения мер ЗИ определяется в соответствие с таблицей 1-7.

Таблица 1-7. Степень внедрения мер ЗИ

Степень внедрения мер ЗИ	Описание
Отсутствует необходимость	Внедрение меры безопасности безосновательно, так как предприняты другие меры, которые уже предоставляют достаточный уровень безопасности для соответствующей угрозы или предлагаемые меры не подходят ситуации

Да	Меры безопасности полностью внедрены и эффективно выполняют свою функцию
Частично	Внедрена часть рекомендуемых мер безопасности
Нет	Меры безопасности не внедрены

Результаты базовой проверки ИБ используются далее в качестве основы для планирования мер ЗИ, которые не реализованы или реализованы не полностью.

Дополнительный анализ ИБ

Цель этого этапа проверить необходимость внедрения дополнительных мер ЗИ. Если в процессе оценки требований ИБ выяснено, что исследуемые объекты (например, приложения или ИТ-системы) требуют высокого или очень высокого уровня защиты, или если для них отсутствуют меры ЗИ в каталогах *IT-Grundschutz*, необходимо провести дополнительный анализ, для внедрения дополнительных мер ЗИ (см. рисунок 1-3).

Для уменьшения затрачиваемых ресурсов на дополнительный анализ ИБ, методология рекомендует концентрироваться на наиболее уязвимых и часто используемых частях ИС. Такими могут являться:

- ИС с высокими требованиями защиты.
- Коммуникационные связи с внешним миром.
- Коммуникационные связи, отвечающие за передачу конфиденциальной информации.
- Коммуникационные связи, на которые накладываются ограничения по типу передаваемой информации.
- Строение и помещения, требующие высокий уровень безопасности.

Подобный подход, с одной стороны, позволяет сузить объем анализируемых сценариев реализации угроз БИ, с другой стороны, может привести к пропуску критичных угроз БИ.

Методы дополнительных проверок:

1. Анализ рисков.

2. Комплексное исследование уязвимостей на сайтах (*web*-приложениях, мобильных приложениях) методом проникновения, обеспечивающее

своевременное выявление угроз, а также снижение ряд экономических и репутационных рисков организации (пентест).

3. Дифференцированный анализ безопасности.

В связи с тем, что успех дополнительной проверки безопасности напрямую определяется квалификацией экспертов, это создает риск субъективности и не гарантирует повторяемость результата. При этом необходимо глубокое знание предметной области членами команды, так как иначе существует высокая вероятность, что некоторые необходимые меры безопасности будут пропущены.

Подготовка списка угроз

Цель данного этапа – составление списка угроз БИ для рассматриваемых в рамках дополнительного анализа ИБ объектов оценки. Для этого рекомендуется уменьшить количество объектов.

В каталогах *IT-Grundschutz* содержится информация о возможных видах угроз БИ для объектов оценки. В первую очередь проводится уменьшение количества рассматриваемых объектов:

1. Из списка рассматриваемых объектов удаляются те объекты, которые не нуждаются в оценке рисков. Эти объекты не участвуют в процессе моделирования. Обычно объекты можно убрать только из модулей 2–5, так как модули 1 уровня обычно относятся к большинству рассматриваемых объектов.

2. Модули, в которых не оказывается объектов оценки после структурного анализа также удаляются.

3. Итогом этих шагов является таблица модулей, содержащих объекты с требованием высокой и очень высокой безопасности.

4. Каждый модуль из *IT-Grundschutz* соотносится со списком угроз из каталога. К каждому модулю добавляется соответствующий список угроз.

5. Производится группировка, сортировка и удаление копий угроз для каждого объекта оценки.

6. К каждому объекту также добавляется список параметров ИБ (кроме объектов 1 уровня).

Определение дополнительных угроз

В определенных случаях у объекта могут существовать дополнительные угрозы БИ (помимо перечисленных в *IT-Grundschutz*), которые не включены Каталог угроз БИ, в том числе:

- угрозы, принадлежащие определенной технологии или приложению;
- угрозы, наносящие урон только в очень специфических ситуациях;
- угрозы, требующие от нападающего высокую квалификацию или большое количество ресурсов.

В процессе определения дополнительных угроз следует учитывать возможность нарушения трех свойств информации – $К, Ц, Д$. Поиск дополнительных угроз БИ производится для тех параметров объекта, которые требуют высокий или очень высокий уровень безопасности. Отметим, что угрозы БИ, приведенные в *IT-Grundschutz,* соответствуют стандартному уровню безопасности. В этой связи вне зависимости от параметров защищаемого объекта необходимо проводить поиск дополнительных угроз БИ для объектов, которые нельзя отнести ни к одному из представленных модулей. Источниками поиска дополнительных угроз БИ являются:

- документация производителя;
- Интернет;
- собственный анализ угроз БИ.

Оценка угроз

По каждой из угроз БИ должны быть проведена проверка и получены оценки соответствия текущих или планируемых меры ЗИ необходимому уровню защищенности информации. Здесь обычно используются меры ЗИ, представленные в каталогах *IT-Grundschutz*. Проверка осуществляется в соответствии со следующими критериями.

1. Полнота, оцениваемая по полноте мер ЗИ от каждой угрозы.

2. Прочность, оцениваемая соответствием мер ЗИ, представленных в каталогах IT-Grundschutz, каждой из угроз БИ.

3. Надежность, оцениваемая объемом затрат на преодоление использованных мер ЗИ.

Результат проверки для каждой угрозы БИ позволяет оценить адекватность текущих и запланированных мер ЗИ против заданной угрозы БИ, или необходимость проведения работы с рисками по этой угрозе.

Работа с рисками

На практике обычно выбирают несколько угроз БИ, для которых предложенные в каталогах *IT-Grundschutz* меры не представляют достаточный уровень защиты, и проводят для них анализ рисков. Итоги дополнительного анализа ИБ документируются. Итоговый отчет доводится до сведения руководства организации и утверждается им. Таким образом, руководство организации принимает на себя ответственность за БИ. После этого идентифицированные меры должны быть интегрированы и консолидированы в бизнес-процессе обеспечения ИБ.

Таблица 1-8. Варианты обработки рисков

Варианты обработки рисков	Описание
Снижение риска (за счет дополнительных мер ЗИ)	Вводятся дополнительные меры ЗИ, благодаря которым убираются негативные эффекты угрозы БИ. Для этого можно использовать дополнительные источники информации: – документация производителя и его службы поддержки; – стандарты и лучшие практики; – другие публикации или сервисы; – опыт сотрудников организации или их партнеров.
Отказ от риска (снижение риска за счет реорганизации)	Угроза БИ исчезает, так как исчезает объект (актив) за счет реорганизации бизнес-процессов или информационных ресурсов. Причины использования подхода: – все доступные контрмеры слишком дороги, но риск угрозы БИ не может остаться без внимания; – реорганизация может принести дополнительную пользу; – все доступные контрмеры создадут ограничения, которые не позволяют комфортно пользоваться системой.
Принятие риска	Угроза БИ и риски, которые она создает позволительны. Причины принятия такого решения: – угроза БИ существует только при определенных, редко случающихся обстоятельствах; – для проблемы нет известных решений; – решение проблемы дороже стоимости защищаемого объекта.
Перенос риска	Решение угрозы БИ передается другой организации. Причины:

	– потенциальные потери – только финансовые; – организация уже планирует передать части системы другой организации; – по коммерческим или техническим причинам лучше передать решение проблемы партнерам.

Базовая проверка безопасности II

Этап аналогичен этапу Базовая проверка безопасности I.

1.2.2. Ограничения методологии *IT-Grundschutz*

Методология *IT-Grundschutz* является гибкой, так как, в отличии от подхода, используемого в законодательстве РФ, позволяет для одних организаций или ИС использовать существующий набор мер ЗИ, определяемый на основе сценариев негативных последствий для активов организации, для других – использовать дополнительный перечень ЗИ , формируемых экспертным путем.

С другой стороны, методология *IT-Grundschutz* сложна в реализации и требует привлечения нескольких экспертов. Экспертный анализ обладает рядом ограничений:

- субъективность;
- отсутствие полноты или избыточность;
- сложная повторяемость процесса.

1.2.3. Методология *ISO 2700x*

Методология *ISO 2700x* и схожих с ней стандартов [13–17] отличается от подхода, используемого в законодательстве РФ и методологии *IT-Grundschutz*. Это проявляется в отсутствии четко определенных требований к системе ИБ, которые предлагается формировать на базе оценки рисков ИБ и вероятности угроз БИ (четкий перечень возможных угроз БИ отсутствует).

Данный подход обеспечивает формирование гибкой МУ, а также точечный, а потому потенциально эффективный, подбор компонентов системы ИБ. При этом вероятность реализации угрозы оценивается, исходя из возможности нарушения $К, Ц, Д$ защищаемой информации из-за наличия уязвимостей системы ИБ ИС. С

другой стороны, подобный подход может привести к пропуску критических угроз ИБ из-за экспертного подхода в определении и оценки угроз БИ и рисков ИБ.

Отметим, что в [13] обеспечение БИ рассматривается в терминологии рисков: риск ИБ – потенциальная угроза эксплуатации уязвимости актива, приводящая к появлению вреда для организации.

Структурная схема методики приведена на рисунке 1-7. Далее этапы методологии менеджмента рисков ИБ рассматриваются более подробно.

Установление контента

Ключевой особенностью стандарта [13] является наличие четко определенной области его применения. В нем определены процессы и ИС организации, которые отнесены к области реализации требований стандарта. К процессам и ИС, оставшимися за рамками стандарта, его требования не применяются, поэтому эта часть ИС организации может оказаться уязвимой для КА. В результате уровень защищенности всей организации может снижаться.

Для реализации повторяемости процесса менеджмента рисков ИБ в [16] на начальном этапе определяется и документируется процесс менеджмента рисков, основные критерии (критерии оценки рисков, принятия риска и критерии оценки воздействия инцидента ИБ). При этом должны быть разработаны критерии, используемые для оценки рисков, и определены их значения. Критерии оценки риска зачастую зависят от политик, намерений, целей организации и интересов причастных сторон. В этой связи организация должна определять собственные шкалы для уровней допустимости риска. При этом учитывается, что:

- критерии оценки риска могут включать ряд пороговых значений, когда указывается желаемый целевой уровень риска, одновременно, при определенных обстоятельствах высшее руководство организации может принимать риски, находящиеся выше этого уровня;
- критерии оценки риска могут выражаться как соотношение количественно оцененной прибыли (или иной выгоды бизнеса) к количественно оцененному риску;

- различные критерии оценки рисков могут применяться к различным классам рисков, например, могут не приниматься риски, связанные с неисполнением законодательно-нормативных требований, в то время как принятие рисков высокого уровня может быть допустимо, если это определено договорным обязательством;
- критерии оценки рисков могут включать требования о проведении в будущем дополнительной обработки риска, например, риск может быть принят, если принято решение и взяты обязательства предпринять меры по его снижению до приемлемого уровня в течение определенного периода времени.

Критерии оценки рисков могут различаться в зависимости от того, насколько долго, (предположительно) риск будет существовать (например, риск может быть связан с временной или кратковременной деятельностью). Критерии оценки риска должны устанавливаться с учетом критериев бизнеса, особенностей законодательно-нормативной среды, социальных и гуманитарных факторов.

Необходимо учитывать:

- свойства ИБ: если один критерий не важен для организации (например, потеря конфиденциальности), то все риски, воздействующие на этот критерий, возможно, не учитывать;
- важность бизнес-процесса или деятельности, поддержанной специфическим активом или устанавливаемый активом: для менее важных бизнес-процессов назначается низкий приоритет рассмотрения рисков и наоборот.

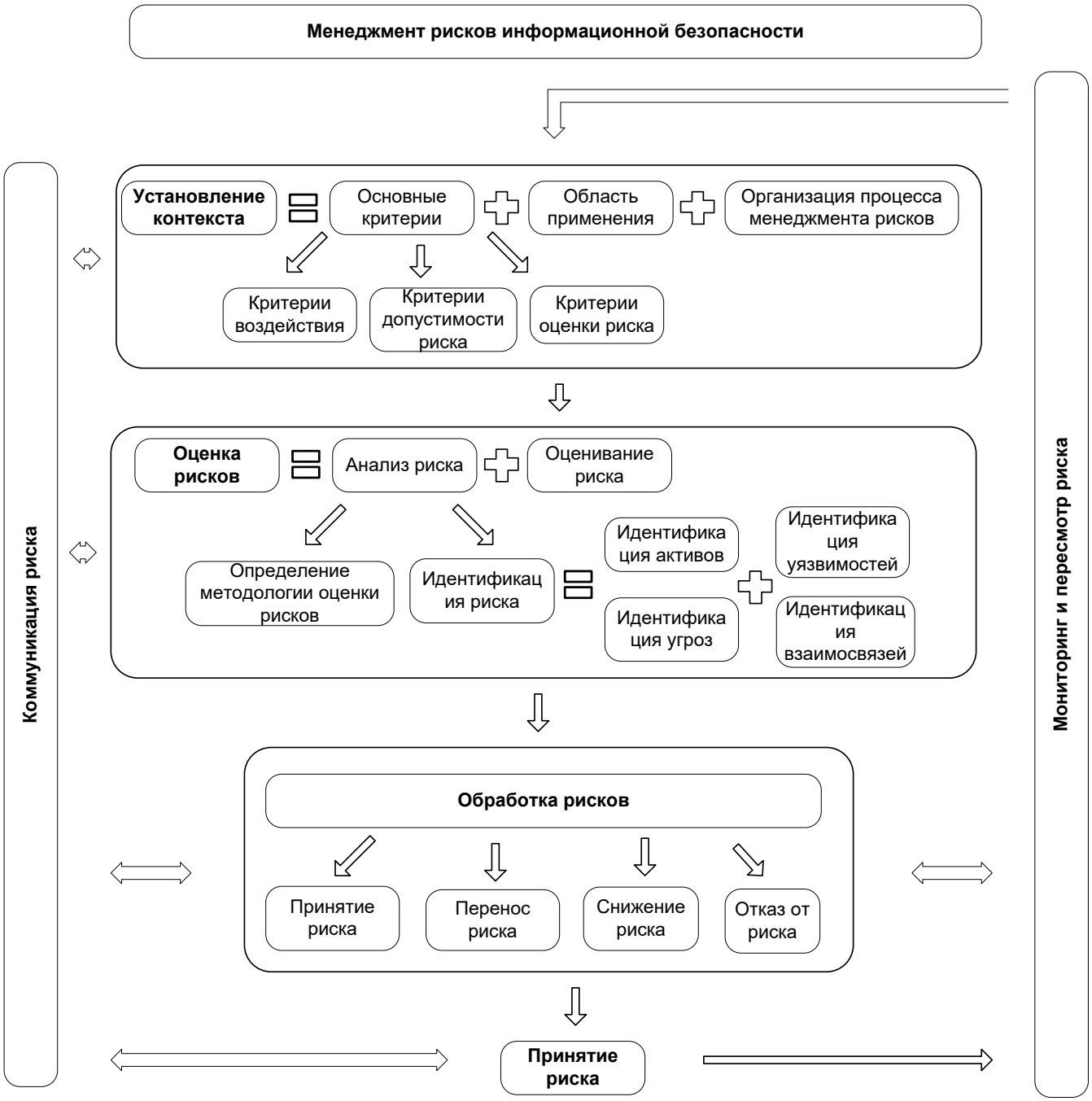

Рисунок 1-7. Структурная схема менеджмента рисков ИБ

Оценка рисков

На этапе оценки рисков проводится формирование перечня рисков ИБ путем их анализа оценки в соответствии с определенной организацией и задокументированной методологией оценки рисков. Для оценки рисков используются качественные, количественные и комбинированные методы [15, 16]. При этом, зачастую, количественная оценка рисков реализуется с помощью введения шкал градации активов и угроз [16]. Также в [15] описан метод

количественной оценки рисков, который следует использовать для оценки частоты эксплуатации уязвимости нарушителями за год и расчета стоимости потерь и влияния на бизнес от каждой КА. Количественная оценка в большинстве случаев использует статистику инцидентов. Таким образом, преимущество количественной оценки рисков – реалистичность; недостаток – ограниченность статистических данных. На практике сначала используется качественная оценка, чтобы получить общую индикацию относительно уровня риска и показать основные риски. Форма анализа должна быть совместима с критериями оценки риска, определенными в организации. Примеры различных методов оценки риска ИБ или подходов приведены в приложении Е стандарта *ISO27001* [16].

$$R = \rho \cdot C_a, \tag{1.13}$$

где

ρ – вероятность реализации угрозы ИБ для актива A организации;

C_a – ценность актива А и уровень ущерба организации вследствие нарушения $К, Ц, Д$ актива A.

Для проведения оценки необходимо идентифицировать риски, выполнив для этого следующую последовательностью действий.

1. Идентификация активов.

Необходимо выделить конкретные активы (люди, информация, сервисы, техника), которые являются критичными в организации. Критичность активов определяет организация самостоятельно.

В прикладных методах анализа рисков обычно рассматриваются следующие классы активов:

- оборудование (физические ресурсы);
- ПО (утилиты и другие вспомогательные программы);
- информационные ресурсы (базы данных, файлы, все виды документации);
- системные интерфейсы (внешние и внутренние возможные соединения);
- люди, которые пользуются и поддерживают ИТ-систему.

Идентификация актива должна быть выполнена на соответствующем уровне детализации, необходимом для оценки риска. Должен быть идентифицирован владелец, который несет ответственность за актив для каждого актива.

2. Идентификация угроз ИБ.

В приложении С стандарта *ISO27001* [16] приведен список классов угроз и подходов к формированию перечня [16]. В *NIST* стандартах [15] предлагается перечень угроз формировать на основе истории КА на организацию, и баз данных, содержащих информацию о КА, например, *NIPC, OIG, FedCIRC*, а также средства массовой информации.

Под угрозой [16] понимается потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам. Угрозы могут иметь естественную или человеческую природу и могут быть случайными или преднамеренными, поэтому должны быть идентифицированы случайные и преднамеренные источники угрозы. Так как некоторые угрозы могут затронуть больше, чем один актив, они могут вызывать различные воздействия в зависимости от того какие затронуты активы.

3. Идентификация существующих требований стандарта, законодательства РФ и партнеров.

В процессе оценки рисков, необходимо учитывать, как собственный опыт и статистику инцидентов ИБ в конкретной области, так и требования законодательства РФ по ИБ и партнеров. Требования обсуждаемого стандарта приведены в приложении А [16]. Сбор статистики реализуется путем ведения журнала регистрации инцидентов, где записывается время обнаружения, данные сотрудника, обнаружившего инцидент, категорию инцидента, затронутые активы, планируемое и фактическое время решения инцидента, а также перечень работ, проведенных для устранения инцидента и его последствий.

Пересмотр требований должен проводиться регулярно, что позволит повышать их эффективность. Существующие или запланированные требования могут быть определены как неэффективные, или недостаточные, или

неоправданные, например, по причинам стоимости. Такие требования должны быть удалены, заменены другими, более подходящим.

4. Идентификация уязвимостей.

В приложении D стандарта [16] приведена таблица с типовыми уязвимостями. После разработки МУ необходимо идентифицировать уязвимости в окружении активов. Уязвимость, у которой нет соответствующей угрозы, возможно, не требует реализации мер ЗИ, однако, уязвимость должна быть распознана и должен проводиться периодический мониторинг ее изменений. Подход к технической оценке уязвимостей приведен в Приложении В.3 [16]. Результатом разработки МУ, модели нарушителя и идентификации уязвимостей является определение сценариев реализации КА, приводящих к нарушению ИБ организации.

Уязвимость может быть идентифицирована в:

- организации;
- внутренних процессах и процедурах организации;
- практике менеджмента организации;
- персонале организации;
- физической среде;
- конфигурации ИС;
- аппаратных средствах, ПО или оборудовании связи;
- зависимости от внешних партнеров.

Отметим, что стандарт *NIST* [17] рекомендует использовать единый перечень уязвимостей *CVE*. При этом отдельное внимание рекомендуется уделять уязвимостям, выявленным на предыдущей итерации по оценке рисков ИБ, из аудиторского отчета, результатов сканирования и тестирований на проникновение, из требований по безопасности (например, *FedCIRC*) и иным базам данных, например, *NIST I-CAT vulnerability database* и *SecurityFocus.com* [15].

После установления взаимосвязей активов, угроз ИБ и уязвимостей проводится анализ рисков. Задача анализа рисков определить ущерб или последствия для организации при реализации КА по определенным выше инцидентным сценариям по (1.13).

В прикладных методах анализа рисков обычно используются следующие подходы к оценке активов C_a:

- стоимость чистого восстановления и замены информации(актива) (если вообще возможно);
- потери организации при компрометации актива, как прямые (неблагоприятное воздействие на бизнес), так и юридические или репутационные;
- нанесение ущерба другим активам.

Вероятность реализации угрозы ИБ ρ для актива A осуществляется с использованием качественных или количественных методик оценки для идентифицированных рисков. При этом учитывается частота возникновения угроз ИБ, а также насколько легко может быть использована данная уязвимость. Для этого может учитываться следующая информация:

- о случаях и соответствующей статистики для вероятности угрозы ИБ;
- для преднамеренных источников угрозы: о мотивации и возможностях нарушителя, ресурсах, доступных для возможных нарушителей, так же как восприятие привлекательности и уязвимости активов для возможного нарушителя;
- для случайных источников угрозы: о географических факторах, например, близость к химическим или нефтяным организациям, возможности критических погодных условий, и факторы, которые могли влиять на человеческие ошибки и сбой оборудования;
- об уязвимостях, как индивидуальных, так и в агрегации;
- о существующих мерах ЗИ и о том, насколько эффективно данные меры снижают вероятность реализации угрозы ИБ.

Обработка рисков

Обработка рисков в соответствие с методологией *ISO* аналогична действиям, описанным в таблице 1-8.

Рассмотрим более подробно процесс принятия риска, который считается приемлемым, когда в рамках оценки рисков стоимость потерь от реализации риска ниже стоимости затрат на защиту или стоимости актива (стоимости потерь организации от реализации риска). Отметим, что при этом компенсирующие меры противодействия принятого риска в стандартах [13, 14, 15] не регламентированы. Таким образом, уровень защищенности организации при использовании международных подходов напрямую зависит от качества экспертизы по оценке рисков и, соответственно, квалификации привлекаемых экспертов.

Мониторинг и пересмотр рисков

Важной особенностью международного подхода является требование по систематической переоценке рисков. Как и любой процесс в рамках СУИБ, процесс оценки рисков должен быть реализован в рамках цикла *PDCA (Plan – Do – Check – Act)*. Отметим, что использование процессного подхода определяет необходимость систематически переоценивать риски, а значит обновлять перечень угроз и уязвимостей ИБ, то есть корректировать систему ИБ. Однако, оценка вероятности угроз и рисков ИБ оказывается краткосрочной, поскольку не учитываются возможные изменения вектора КА в течение времени (прогнозирование). В результате «мгновенные» оценки вероятности угроз ИБ и соответствующих рисков для ИС, оказавшиеся относительно высокими в конкретный момент времени, в дальнейшем могут оказаться не состоятельными. Действительно, нарушитель, будучи необнаруженным, имеет возможность в течение длительного времени собирать информацию о средствах защиты внешнего и внутреннего периметра ИС и готовить результативную КА. Таким образом, разработка подходов, обеспечивающих получение динамических оценок вероятности угроз ИБ и соответствующих рисков ИБ для ИС, являются актуальным.

1.2.4. Ограничения методологии *ISO*

При оценке рисков методология *ISO* рекомендует учитывать ценность активов организации. Однако нарушитель, в отличие от сотрудников организации, не знает реальной ценности активов, поэтому он может оперировать только предполагаемой величиной и потенциальной величиной выгоды, которую может получить (например, выплата за расшифровку данных после КА с помощью шифровальщика). Следовательно, потерянная ценность актива для организации в ходе успешной КА нарушителем не равна выгоде, получаемой нарушителем.

Ограничение области применения методология *ISO* приводит к появлению процессов и ИС, оставшимися за рамками стандарта, поэтому они могут оказаться уязвимыми для КА. В результате уровень защищенность всей организации может снизиться. Гибкий подход в формировании методики оценки рисков, в частности, уровней допустимости риска и возможности принятия рисков высшим руководством организации, находящихся выше допустимого порога, может привезти к формальному выполнению требований стандарта и отсутствию необходимых мер ЗИ, так как требования к стандартизации по методологии *ISO* являются обязательными для работы с крупными международными организациями.

Экспертный подход в формировании перечня и оценки вероятности угроз ИБ может привести к пропуску критических угроз ИБ, не корректной оценки угроз БИ и рисков ИБ. Для эффективной реализации процесса международный стандарт предусматривает привлечение такого количества специалистов, чтобы в процессе управления рисков было задействовано не менее 13 ролей [15]. На практике данное условие сложно выполнить. Таким образом, человеческий фактор в экспертном подходе создает риск субъективности и не гарантирует повторяемость результата.

1.3. Анализ научных подходов к определению и прогнозированию компьютерных атак

Взаимно однозначное соответсвие между терминами КА и угрозами БИ обосновано в [5]. В этой связи, далее будем использовать термин КА. В настоящее время отечественными и зарубежными специалистами в области обеспечения ИБ проводятся активные исследования с целью определения и прогнозирования возможных векторов КА, что подтверждают результаты информационного поиска открытых отечественных и зарубежных публикаций за последние 10 лет [18–44, 56–88], представленные в приложении D.

Из таблицы, представленной в приложении D видно:

1. В большинстве российских научных исследований по оценки рисков ИБ [24, 25, 30, 31, 56–58, 62–68, 77–79, 86, 87] авторы используют методологию оценки угроз (рисков) ИБ законодательства РФ [1–5, 52] и международного стандарта *ISO 27005* [16], предлагая использовать на этапе оценки угроз (рисков) ИБ различные математические методы: теорию графов [18–20, 62, 64, 66], байесовский подход [56, 63], метод рандомизированных сводных показателей [57], метод статистических показателей [19], метод экспертных оценок (например, *OCTAVE* [24, 25, 30, 31, 58, 78, 79, 86, 87]), метод анализа иерархий [66], матрицу Мак–Кинзи [65], количественные методы [68], деревья решений [77]. При этом в большинстве исследований угрозы (риски) ИБ рассматриваются с точки зрения организации. Оценка рисков с учетом мотивов и критериев нарушителя представлена только в работе [78]. При этом в работе [78] отсутствует обоснование выбранных критериев и методик оценивания их значений.

2. Задача оптимизации перечня угроз ИБ и подходы к ее решению обсуждаются в [59, 62, 64, 67, 77]. Отметим, что в большинстве работ классы угроз ИБ выделяются, в предположении об использовании единственного способа защиты от данного класса КА. Альтернативный вариант оптимизации перечня угроз ИБ предложен в работе [64]. Здесь для разделения механизмов защиты на

типы и анализ остаточных рисков ИБ авторы предлагаю использовать ориентированный граф и систему уравнений Колмогорова.

3. Подходы, обеспечивающие возможностью учета динамического изменения во времени перечня угроз ИБ, рассматриваются в [18, 63, 66, 67, 79]. Например, в работе [66] предложено оценку рисков проводить на основе неструктурированных данных, полученных из Интернета, однако, к сожалению, не конкретизированы источники, а также информация, которую необходимо учитывать, что может привести к подучению некорректной оценки. Также отметим, что в [66] не анализируется и не рассматривается, собственно, нарушитель.

4. Большинство российских научных исследований по оценки рисков ИБ носит теоретический характер. В большинстве исследований не определены источники статистических и экспертных данных, которые нужно использовать для практической реализации. Зачастую апробация методик реализуется на теоретических данных. Использование реальных исходных данных о событиях ИБ предлагается только в нескольких работах [19, 34, 63, 66, 67]. Отметим, что при этом требования к исходным данным не предъявляются. В этой ситуации существует высокая вероятность пропуска КА нулевого дня, или КА, обнаружение которой имеющимися средствами ЗИ оказывается невозможной.

5. В иностранных исследованиях по оценке рисков ИБ [22, 23, 29, 37, 59–61, 69, 70, 71–76, 80–85] авторы зачастую рассматривают частные задачи по оценке рисков ИБ, в том числе:

– подходы по повышению эффективности экспертного метода оценки рисков ИБ (например, для повышения эффективности экспертной оценки предлагается использовать средства автоматизации для извлечения информации из базы знаний [70], методы формирования экспертных групп и этапов оценки рисков ИБ (*VECTOR, OCTAVE, CRAMM, FRAP, SVIDT, CORAS, MSAT* и *NIST SP800-30*) [27, 29, 58, 60, 71, 76, 80, 86]), ограничения и сравнительный анализ которых проведен только в [71], при этом, однако, не были получены оценки эффективности данных методов.

– способы оптимизации расчетов по оценке рисков ИБ с помощью численных методов и средств автоматизации [27, 70, 81, 82] (ограничения методологий оценки рисков ИБ, описанные в разделе 1.2 при этом сохраняются);
– способы оптимизации формирования перечня угроз ИБ с помощью теории графов [26, 61, 69, 83] и деревьев КА [26, 70, 85], которые оказываются несвободными от известных недостатков (см. Таблица 1-9);

Таблица 1-9. Преимущества и недостатки подходов по оптимизации перечня угроз ИБ

Преимущества подходов по оптимизации формирования перечня угроз ИБ	Недостатки подходов по оптимизации формирования перечня угроз ИБ
– обеспечивает наглядное, простое и ясное графическое представление; – ориентирована на средства управления, направленные на предупреждение и/или уменьшение последствий опасных событий, и оценку их эффективности; – может быть применена в отношении благоприятных последствий; – не требует специальных навыков для реализации.	– не позволяют отображать совокупности причин, возникающих одновременно и вызывающих последствия (случай, когда в дереве неисправностей, отражающем левую сторону диаграммы, находится логический элемент "И"); – представляют сложные ситуации в чрезмерно упрощенном виде, особенно при применении количественной оценки; – не позволяет учесть изменение во времени.

– разрабатывают динамические модели противоборства нарушителя и специалиста по ИБ на основе методов теории игр [28, 37, 74, 83], которые обеспечивают возможность анализа динамики процессов вторжения, противодействия и восстановления уровня ИБ и соответствующего уровня риска реализации для конкретной КА, в которых используются не реальная информация о совершенных атаках, но экспертные оценки, что не позволяет прогнозировать вектор возможных КА на организацию;
– создают модели, учитывающие изменение вероятности реализации проводимой КА во времени [37, 69, 72–74] (например, в [69, 75] представлена взаимосвязь КА и компонентов инфраструктуры организации с возможностью в режиме реального времени определить меры ЗИ; в [84] предложен механизм обнаружения КА, с помощью машинного обучения – выявление аномального отклонения поведения

пользователя от вектора поведения пользователя, который, однако, обеспечивает в режиме реального времени обнаружение КА, но не ее предсказание; в [73] проведена аналогия между системой ЗИ и иммунной системой человека; в [72] предложена формула расчета риска угрозы успешной реализации КА, учитывающая изменение КА во времени, что позволяет оценить изменение вероятности успеха реализации проводимой КА во времени и дать прогноз значения критического времени для анализа ситуации и принятия решений для данной конфигурации инфраструктуры ИБ организации, однако не позволяет спрогнозировать потенциальный вектор КА), при этом, однако, исследуются процессы и этапы реализации конкретной КА, но не прогнозируются дальнейшие сценарии развития (например, не учитываются причины выбора методов и объектов КА).

6. Существуют подходы, направленные на формирования профиля защиты для конкретного типа объекта защиты (корпоративных ИС, информационно-коммуникационных систем и др.) [18–20, 22–28, 29–31, 62] или учета свойств информации [19, 21], которые позволяют учитывать специфику объекта защиты, снижать затраты на анализ, время и ресурсы. Отметим, что данному подходу присущи ограничения российской нормативно-правовой базы, описанные в разделе 1.1, который также не предусматривает рассмотрение особенностей угроз ИБ, обусловленных особенностями взаимодействия объектов защиты организации.

7. Известны подходы, используемые для разработки модели нарушителя, рассматриваются в [22, 82] (например, в [22] обосновано, что для оценки угроз и рисков ИБ необходимо учитывать возможности, намерения и цели нарушителя. Однако данные о нарушителе, как и в законодательстве РФ, учитываются скорее качественно (с помощью таблицы градаций, значение и которых определяет эксперт), но не количественно. В [82] предложено учитывать учет мотивацию нарушителя, но критерии выбора или принятия решений в работе не представлены, поэтому их выбор остается за экспертом в области ИБ).

8. Потенциальные методы проведения и объектов КА рассматриваются в [32–35]. Здесь проводится анализ форумов *DarkNet,* но не данных, полученных организацией или экспертами. Необходимо отметить, известную ограниченность данных исследований, в которых используется только число упоминаний в *DarkNet* данного метода реализации КА и число попыток реализации КА на организацию, а также отсутствие методологии использования данной информации. Необходимо отметить работу [35], в котором предложено использовать теорию З. Фрейда (1901 г.), в которой обоснована возможность выявления скрытых намерений человека на основе допускаемых им оговорок. Для этого ее авторы предлагают анализировать форумы *DarkNet* с помощью методов *DER, SentiStrenght* и *LIWC15*. Данный подход (эффективность которого по оценкам авторов составила 36%) позволяет учитывать при прогнозировании вектора КА не только факт обсуждения метода, но и эмоциональную окраску соответствующего обсуждения.

9. Возможность использования методов социальной инженерии для проведения КА обоснована в [33]. Здесь показано, что анализ личной информации и поведения пользователей в социальных сетях позволяет выявить потенциальных жертв социальной инженерии среди сотрудников организации. Предложенный подход позволяет для каждого пользователя оценить вероятность его использования нарушителем для проведения КА и проинформировать пользователей и руководителей организации о соответствующих рисках. Отметим, что в [33] не описана методика идентификации сотрудника и его профиля в социальной сети, без которой получение достаточного объема исходных данных оказывается затруднительны, а также не представлены модель нарушителя и обоснование набора методов социальной инженерии, используемых нарушителем для извлечения информации из социальных сетей, используемой далее для реализации КА. В этой связи оценить эффективность методов для противодействия данного типа КА не представляется возможным.

10. Методы прогнозирования новых уязвимостей ПО в обновленных версиях ПО (ОС, браузерах, офисных приложениях и др.), основанные на анализе

накопленной информации о количестве уязвимостей и их типах в их предыдущих версиях, изучались в [36–44]. В этих работах проводился анализ зависимостей числа уязвимостей от номера версии (аналоги временных рядов) с помощью одинарного, двойного и тройного экспоненциального сглаживания [36–38], статистических методов (Кростона, *ARIMA*) [36, 39, 40], кластерного анализа [41, 42], нейронных сетей [36, 43] и машинного обучения [36, 43, 44], оценка эффективности которых проводилось на основе сравнения известных и спрогнозированных значений числа уязвимостей ПО. Для этого вычислялись средняя абсолютная и среднеквадратическая ошибки отклонений спрогнозированных значений от их известных из статистических данных фактических значений [36]. При этом не было получено универсального аналитического выражения для функция, используя которую можно прогнозировать число новых уязвимостей в данном ПО, так как выбор метода прогнозирования и точность прогнозирования зависят от типа ПО и/или ОС [36], что затрудняет их сравнительный анализ. Отметим, что ограничение области анализа уязвимостей ИБ поиском только уязвимых частей программного кода (например, элементов взаимодействия с внешними системами, пользовательских интерфейсов) позволяет несколько (однако, не кардинально) улучшить качество прогнозирования новых уязвимостей [44]. В этой связи для улучшения точности прогнозирования новых уязвимостей ИБ на основе имеющейся статистики выявленных ранее уязвимостей ИБ представляется целесообразной разработка методов прогнозирования уязвимостей ИБ, в которых учитываются цели, мотивы и квалификация.

11. Анализ подходов к прогнозированию возможного вектора КА на новую архитектуру системы ИБ на основе использования ВПО проведен в [32]. (Отметим, что по оценкам [32], количество совершенно нового ВПО, появившегося в период с 3 квартала 2016 г. по 2 квартал 2018 г., составило менее 10% от общего числа ВПО.) Оказалось, что что данный тип ПО легко масштабируется, адаптируясь к различной инфраструктуре системы ИБ. Это дает возможность успешно применять старые вектора КА для новой архитектуры

(например, для облачных технологий и Интернета вещей (*internet of things (IoT)*). Классификация известного ВПО, а также методика проверки возможности его адаптивности к новой инфраструктуре представлены в [32]. Однако здесь не описаны практические результаты, подтверждающие работоспособность данной методики. Также отметим, что обсуждаемый подход имеет очевидное ограничение, так как здесь не учитываются мотивы нарушителя и, соответственно, его заинтересованность в доработке того или иного ВПО и его использовании для реализации КА на ИС конкретной организации.

12. Оценки эффективности и работоспособности изученных методик прогнозирования угроз ИБ получены только в [57, 78, 79, 82], что определяет необходимость проведения их дальнейших исследований.

1.4. Постановка задач исследования

Анализ действующей нормативно-правовой базы в области ИБ, соответствующих научных исследований, в том числе посвященных разработке методов расчета вероятности угроз на основе нормативных документов ФСТЭК России и ФСБ России, методов оценки рисков ИБ на базе международных стандартов, методов по оптимизации оценки рисков ИБ, прогнозированию уязвимостей, угроз ИБ и методов КА, исследуемых в научных работах позволяют сделать обоснованный вывод об отсутствии единого метода прогнозирования наиболее вероятных векторов КА и соответствующих математических моделей. Это подтверждается:

- аналитическими отчетами российских специалистов (см, Паспорт федерального проекта «Информационная безопасность» [89]);
- аналитическими отчетами зарубежных специалистов («Отчет Всемирного экономического форума по глобальным рискам» [90]);
- результатами соревнований по кибербезопасности между командами атакующих, защитников и специалистов в области мониторинга ИБ (например, *PHDays* [91, 92]).

Ключевыми ограничениями существующих методологий по формированию модели угроз и оценки рисков ИБ являются:

- отсутствие методов оценивания динамики вероятных изменений векторов КА;
- рассмотрение объекта КА и угрозы/риска ИБ с точки зрения организации/оператора/владельца или требований нормативных документов, но не с точки зрения нарушителя. С одной стороны, это приводит к недостаточной защищенности и потерям организации из-за КА, а с другой стороны к не эффективному расходованию ресурсов организации (как финансовых, так и человеческих);
- используют экспертные и численные методы оценки значений параметров, использующихся для вычисления вероятности угроз и рисков ИБ.

Известные методики формирования модели угроз и оценки рисков ИБ обеспечивают получение оценок угроз БИ только в конкретный момент времени – «мгновенные» оценки вероятности угроз ИБ и соответствующих рисков для ИС, которые, однако, с неизбежностью изменяются с течением времени. Так как, например, нарушитель, совершивший успешную КА, будучи необнаруженным, имеет возможность в течение длительного времени собирать информацию о средствах защиты внешнего и внутреннего периметра ИС и готовить следующую результативную КА.

Использование экспертного подхода при оценке вероятности угроз и рисков ИБ приводит к появлению следующих ограничений:

- субъективность;
- отсутствие полноты или избыточность;
- сложная повторяемость процесса.

Оценка вероятности угроз ИБ и рисков ИБ в современной методологии осуществляется с точки зрения владельца информации/актива, но не с точки зрения нарушителя. Данный недостаток присущ как соответствующим подходам,

основанным на действующем законодательстве РФ, рекомендующем при формировании системы ИБ строить модели нарушителей и модели угроз ИБ на базе ограниченного набора, так и основанным на международном подходе, в соответствие с которым вероятность реализации угрозы оценивается исходя из возможности нарушения $К, Ц, Д$ защищаемой информации из-за наличия угроз и уязвимостей в ИС. Таким образом, модель нарушителя, используемая в методиках, строится на базе экспертной оценки и ограниченного набора типов нарушителей без учета реальных данных о целях и мотивах нарушителей, методах реализации КА, известных им. В то время как такие ключевые факторы КА, определяемые в первую очередь нарушителем, такие как мотив нарушителя, вероятность разоблачения и неизбежности наказания не учитываются.

Существующие научные наработки и исследования по анализу КА:

– нацелены на оптимизацию существующих международных стандартов и нормативно-правовых документов по ИБ путем автоматизации, наглядного и упрощенного представления, формирования профилей ЗИ для конкретных типов объектов и повышения эффективности экспертной оценки с помощью специальных методов ее проведения;

– имеют узкий прикладной характер по анализу КА после начала практической стадии ее реализации: обнаружение, динамика развития и противодействие;

– сводятся к задачам сбора и приведения к единому виду информации об инцидентах ИБ и вновь разрабатываемых или обсуждаемых на форумах *DarkNet* КА. Прогнозирование вектора КА на базе этих данных учитывает только частоту упоминаний и эмоциональную окраску обсуждений;

– не позволяют сформулировать единый подход к решению вопроса для различного класса ИС и организаций;

– проводятся без оценки эффективности и практической применимости.

Таким образом, актуальна задача изучения взаимосвязи между вектором КА и ключевыми факторами КА, в том числе:

- возможностью КА, включающей в себя критерии выбора объекта КА нарушителем, этапы и методы реализации КА, методами получения информации об объекте, навыками нарушителя;
- ожидаемой полезностью КА, включающе в себя мотивы нарушителя, принципы принятие решения о проведении/продолжении/прекращении КА нарушителем.

Цель диссертационного исследования состоит в разработке математических моделей для прогнозирования вектора КА с точки зрения нарушителя и методики их практического использования.

Для достижения цели диссертационного исследования требуется решить следующие задачи:

1. Обоснование базовых принципов и подходов к построению математической модели принятия решения нарушителем о проведении КА и математической модели, описывающей динамику КА, в которых учитываются мотивы нарушителя, а также принципы принятия решения нарушителем о проведении/продолжении/прекращении КА.

2. Разработка математической модели принятия решения нарушителем о проведении КА и разработка математической модели, описывающей динамику изменения вектора КА во времени и идентификация параметров этих моделей.

3. Разработка методики прогнозирования динамики КА, основанной на использовании предложенных математических моделей, и подтверждение ее работоспособности.

Глава 2. Разработка математической модели принятия решения нарушителем о проведении компьютерной атаки и математической модели, описывающей динамику компьютерной атаки во времени

2.1. Базовые принципы и подходы к построению математических моделей, описывающих принятие решения нарушителем о проведении компьютерной атаки и ее динамику

Анализ существующих подходов к анализу и прогнозированию КА, проведенный в главе 1, показал, что:

- вероятность реализации КА оценивается с точки зрения тяжести последствий для организации;
- при оценке вероятности КА не учитывается изменение с течением времени условий для ее проведения;
- при построении систем защиты ИБ используют ограниченный набор вариантов возможных векторов КА.

Как следствие, модель, описывающая угрозы КА, строится, с точки зрения организации, основываясь на статистической матрице усредненных векторов КА. При этом оценка вероятности угроз ИБ оказывается краткосрочной, так как не учитываются возможные изменения вектора КА в течение времени. В результате «мгновенные» оценки вероятности угроз ИБ и соответствующих рисков для ИС, оказавшиеся не высокими в данный момент времени, в дальнейшем могут оказаться не состоятельными, поскольку нарушитель, будучи необнаруженным, имеет возможность в течение длительного времени собирать информацию о средствах защиты внешнего и внутреннего периметра ИС и готовить результативную КА [93–95].

Напомним, что КА, представляющая собой «целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной ИС или получение несанкционированного доступа к ним с

применением программных или программно-аппаратных средств» [96], определяется нарушителем, который в соответствие с методикой ФСТЭК России [5] является основным источником угрозы ИБ. Действительно, нарушитель определяет на какую информацию и какие ИС будет оказываться целенаправленное несанкционированное воздействие, а также какие методы и средства будут при этом использоваться. Следовательно, модель, описывающую динамику угроз КА, необходимо строить с точки зрения нарушителя.

Сложность построения модели, описывающей динамику КА с точки зрения нарушителя, заключается в том, что вероятность КА в рассматриваемом случае оказывается зависящей от различных факторов КА:

1. Факторы, связанные с нарушителем:

- мотивы нарушителя;
- критерии выбора объекта КА нарушителем;
- этапы и методы реализации КА;
- методы получения информации об объекте КА;
- принципы принятие решения о проведении/продолжении/прекращении КА нарушителем.

2. Факторы, обусловленные изменения во времени условий проведения КА:

- типа, характера и навыков нарушителя;
- компонентов, архитектуры и настроек защищаемой ИС;
- компетенций сотрудников, как рядовых, так и привилегированных.

Решение задачи выбора функции, описывающей зависимость вероятности атаки от ключевых факторов атаки на систему ИБ организации, существенно осложняется необходимостью одновременного учета большого числа разнородных факторов, от которых зависит оцениваемая вероятность. В этой связи представляется целесообразным использовать системный подход, рекомендующий в подобных ситуациях проводить анализ структуры факторов и их группировку. Для формализации функциональных зависимостей между вероятностью атаки на систему ИБ организации и учитываемыми ключевыми

факторами будем использовать опыт, накопленный в экономической и финансовой сферах [97, 98], а также при предупреждении преступлений общей практики [45].

Экономические подходы к анализу мотивов преступников обоснованы Ч. Беккариа и И. Бентама в ТПК [45–47]. Ее суть состоит в том, что любой человек, потенциально, может стать нарушителем при выполнении следующих условий:

1. Наличия возможности совершения преступления.

2. Получения в случае совершения преступления достаточной (с точки зрения нарушителя) полезности.

В ТПК условие совершения преступления сформулировано в виде следующего условия: «если ожидаемая полезность от преступления превышает полезность от иной деятельности, на которое были бы затрачены те же силы и время, то нарушитель совершит преступление». Следовательно, в соответствие с ТПК КА реализуется нарушителем в тех случаях, когда, одновременно, имеется возможность реализации КА и ожидаемая полезность КА с точки зрения нарушителя оказывается достаточной. Следовательно, вероятность реализации КА вида «*A*», реализуемой нарушителем, можно оценить, как условную вероятность достаточности ожидаемой полезности КА при наличии возможности проведения КА, рассчитываемую по формуле:

$$P(EUA) = P(EU|A)\ P(A), \tag{2.1}$$

где

$P(EUA)$ – вероятность достаточности ожидаемой полезности КА вида «*A*» с точки зрения нарушителя;

$P(A)$ – вероятность наличия возможности реализации нарушителем КА вида «*A*»;

$P(EU|A)$ – условная вероятность ожидаемой полезности КА вида «*A*» с точки зрения нарушителя, при оценивании которой учитывается возможность проведения незаметной КА.

Сумма вероятностей достаточности ожидаемой полезности всего перечня рассматриваемых КА с точки зрения нарушителя равна единице. Следовательно, в соответствие с ТПК ключевые факторы можно сгруппировать в два фактора КА:

- возможность проведения КА, определяемая критериями выбора объекта КА нарушителем, этапами и методами реализации КА, методами получения информации об КА, навыками нарушителя, рентабельностью проведения КА;
- ожидаемая полезность КА, включающую в себя мотивы нарушителя, принципы принятие решения о проведении/продолжении/прекращении КА нарушителем.

Таким образом, математическая модель КА должна включать в себя:

- математическую модель принятия решения нарушителем о проведении КА, в которой учтены мотивы нарушителя и принципы принятия решения о проведении/продолжении/прекращении КА;
- математическую модель развития КА во времени, включающую в себя критерии выбора объекта КА нарушителем, этапы и методы реализации КА, методы получения информации об объекте.

Для построения математической модели принятия решения нарушителем о проведении КА, требуется соответствующая модернизация функции ожидаемой полезности, используемой в ТПК, на основе использования которой целесообразно проводить расчет вероятности достаточности ожидаемой полезности КА с точки зрения нарушителя. В этой связи далее проводится анализ зависимости КА от параметров функции ожидаемой полезности, обосновывается возможность использования данных из общедоступных источников информации и обосновывается перечень данных источников.

Для построения математической модели развития КА во времени будем использовать ТДИ, которая, как будет показано далее, позволяет обосновать вид функции, описывающей динамику КА во времени, и методику определения ее параметров. Для этого будут выделены этапы КА с точки зрения нарушителя, определены источники получения нарушителем информации о методах КА, а

также для оценки адекватности математической модели проведены экспериментальные исследования развития КА. Отметим, что при построении математической модели развития КА во времени необходимо учитывать, что длительность КА может достигать нескольких месяцев, в течение которых навыки нарушителя могут быть существенно улучшены.

2.2. Разработка математической модели принятия решения нарушителем о проведении компьютерной атаки

Рассмотрим условную вероятность достаточности ожидаемой полезности КА для нарушителя, включающую в себя мотивы нарушителя, принципы принятие решения о проведении/продолжении/прекращении КА нарушителем.

2.2.1. Функция ожидаемой полезности компьютерной атаки

Ожидаемая полезность – это ценность выгоды от КА, зависящая не от конкретной выгоды, а от дополнительной единицы выгоды. Дополнительная единица выгоды – это выгода нарушителя в единицу времени, полученная им в дополнение к ранее приобретенной выгоде. В соответствии с законом Госсена [99] полезность от каждой дополнительной единицы выгоды сокращается, так как человек приходит к состоянию насыщения. Далее будем использовать это утверждение, учитывая при этом, что нарушитель является среднестатистическим человеком не склонным к риску.

Функция ожидаемой полезности, определенная в ТПК [45–47, 97, 98], с учетом описанных выше особенностей КА и преступлений в информационной сфере, может быть записана в следующем виде:

$$EU = (1-\rho_n)U\left(W_m + W_j\right) + \rho_n U\left(W_m + W_j - F\right), \qquad (2.2)$$

где $U(\xi)$ – функция полезности, определенная ниже;

ρ_n – вероятность разоблачения нарушителя (соответственно, вероятность проведения незаметной КА $\rho_m = 1-\rho_n$);

W_m – выгода (прибль) нарушителя в случае успешной реализации КА, с учетом затрат на реализацию КА, определяемая по формуле $W_m = W_{mpj} - C_j$;

C_j – стоимость использованного метода КА;

W_{mpj} – выручка нарушителя в случае успешной реализации КА;

W_j – текущий доход нарушителя от легальной деятельности;

F – тяжесть наказания в случае разоблачения нарушителя (в денежном эквиваленте).

В качестве функции полезности $U(\xi)$ в ТПК для нарушителя, не склонного к риску, традиционно, используют классическую функцию, предложенную Бернулли [47]:

$$U(\xi) = b \ln\left(\frac{a+\xi}{a}\right), \tag{2.3}$$

где a, b – константы.

Для описания изменения значения выгоды от КА на временном интервале $[t_0, t_0 + t]$, где $t \geq 0$, в терминах ТПК будем использовать формулу Эрлиха [100]:

$$W(t - t_0) = W_0 + W_m(t - t_0) + W_j(t - t_0) - F(t - t_0), \tag{2.4}$$

где

t_0 – момент времени, в который нарушитель принял решение о начале подготовки к реализации КА;

W_0 – благосостояние нарушителя в момент времени t_0;

$W_m(t - t_0)$ – выгода нарушителя в случае успешной реализации КА в момент времени t, отсчитываемое от момента времени t_0 в общем случае:

$$t = t_0 + t_m + t_j + t_c, \tag{2.5}$$

где

t_m – время, потраченное на подготовку и реализацию КА;

t_j – время, потраченное в период времени $[t_0, t]$ на легальную деятельность;

t_c – время, потраченное в период времени $[t_0, t]$ на потребление (досуг, отдых и т.п.);

$W_j(t - t_0)$ – доход нарушителя от легальной деятельности за период времени $[t_0, t]$;

$F(t - t_0)$ – тяжесть наказания в случае разоблачения нарушителя (в денежном эквиваленте) за период времени $[t_0, t]$.

Максимальное значение функции, описывающей зависимость ожидаемой полезности от времени, находится из условия $\frac{dEU(t)}{dt} = 0.$

2.2.2. Анализ функции ожидаемой полезности

Будем считать, что нарушитель системы ИБ, как любой рациональный человек, стремится максимизировать ожидаемую полезность от проведенной КА. Следовательно, в предположении о том, что значения всех за исключением одной переменной c в (2.2) известны, значение

$$c = \arg\max U(c)$$

есть решение уравнения:

$$\frac{\partial EU(c)}{\partial c} = 0. \tag{2.6}$$

Для анализа зависимости функции (2.2) от параметров ρ_n, W_m, F используем эластичность функции, представляющую собой предел отношения относительного изменения значения функции к относительному изменению переменной, когда последнее стремится к нулю [101]:

$$\eta_c^{EU} = \lim_{c \to 0} \left(\frac{\Delta EU}{EU} : \frac{\Delta c}{c} \right) = \frac{c}{EU} \lim_{\Delta c \to 0} \frac{\Delta EU}{\Delta c} = c \frac{\partial EU / \partial c}{EU}, \tag{2.7}$$

Выбор данной характеристики обусловлен тем, что по ее значению можно оценивать степень зависимости вероятности принятия нарушителем решения о

проведении КА от вероятности разоблачения нарушителя ρ_n и тяжести наказания F.

Подставляя (2.2) в (2.7), находим абсолютную величину эластичности ожидаемой полезности от вероятности разоблачения нарушителя ρ_n:

$$\left|\eta_{\rho_n}^{EU}\right| = \left|\rho_n \frac{\partial EU / \partial \rho_n}{EU}\right| = \left|\frac{U\left(W_m + W_j - F\right) - U\left(W_m + W_j\right)}{EU}\right| = \left|\frac{\rho_n F}{EU}\right| \left|\frac{U\left(W_m + W_j - F\right) - U\left(W_m + W_j\right)}{F}\right| \tag{2.8}$$

и абсолютную величину эластичности ожидаемой полезности от тяжести наказания:

$$\left|\eta_F^{EU}\right| = \left|F \frac{\partial EU / \partial F}{EU}\right| = \left|\frac{U'\left(W_m + W_j - F\right)}{EU}\right| = \left|\frac{\rho_n F}{EU}\right| \left|U'\left(W_m + W_j - F\right)\right|. \tag{2.9}$$

Из (2.8), (2.9) видно, что $\left|\eta_{\rho_n}^{EU}\right|$, $\left|\eta_F^{EU}\right|$ с точностью до множителя $\left|\rho_n F / EU\right|$ равняются тангенсу угла наклона прямой, соединяющей точки $U\left(W_m + W_j - F\right)$ и $U\left(W_m + W_i\right)$, и тангенсу угла наклона касательной к графику функции $U\left(W_m, W_j, F\right)$ в точке $W_m + W_j - F$, соответственно. Следовательно, $\left|\eta_{\rho_n}^{EU}\right| > \left|\eta_F^{EU}\right|$, когда $U''(W_m - F) > 0$, т.е. функция возрастает ускоренно, и $\left|\eta_{\rho_n}^{EU}\right| < \left|\eta_F^{EU}\right|$, когда $U''(W_m - F) < 0$, т.е. функция возрастает замедленно.

Из (2.3) так же видно, что в случае нарушителя, не склонного к риску, эластичность ожидаемой полезности от вероятности разоблачения меньше эластичности ожидаемой полезности от тяжести наказания. Это означает, что для нарушителя, не склонного к риску, тяжесть наказания является более существенным сдерживающим фактором, в то время как для нарушителя, склонного к риску, при принятии решения об КА более существенным фактором оказывается вероятность наказания. Отметим, что на практике можно реализовать дифференцированный контроль склонности к риску внутренних нарушителей, являющихся сотрудниками данной организации. Для этого можно использовать

одну из известных методик, например, *HCR-20 («Historical Clinical Risk»), PCL («Psychopathy Checklist»),* имеющей несколько различных модификаций, *VRAG («Violence Risk Appraisal Guide»)* или тест *RSK* Шуберта [102].

Абсолютные величины эластичности ожидаемой полезности от выгоды нарушителя и эластичности ожидаемой полезности от дохода нарушителя от легальной деятельности вычисляются по соответствующим формулам:

$$\left|\eta_{W_m}^{EU}\right| = \left|W_m \frac{dEU/dW_m}{EU}\right| = \left|W_m \frac{(1-p_n)U'\left(W_m+W_j\right)+p_nU'\left(W_m+W_j-F\right)}{EU}\right|, \quad (2.10)$$

$$\left|\eta_{W_i}^{EU}\right| = \left|W_i \frac{dEU/dW_j}{EU}\right| = \left|W_j \frac{(1-p_n)U'\left(W_m+W_j\right)+p_nU'\left(W_m+W_j-F\right)}{EU}\right|. \quad (2.11)$$

Из (2.10), (2.11) видно, что ожидаемая полезность КА, в первую очередь, определяется выгодой нарушителя в случае успешной реализации КА W_m, если текущей доход нарушителя от легальной деятельности меньше выгоды нарушителя от реализации КА, т.е. $W_m > W_j$. Результаты проведенного анализа подтверждаются доступными статистическими данными [103, 104], анализ которых показал:

– большую часть КА осуществляют преступные кибергрупировки, которые работают длительное время [104], легальный доход которых близок к нулю;

– по данным прокуратуры наибольшее число задержанных за КА нарушителей – это люди со средним образованием или студенты, не имеющие постоянного заработка [103, 104].

В том случае, когда доходы от легальной деятельности нарушителя существенно больше выгоды нарушителя в случае успешной реализации КА $\left(W_j > W_m\right)$ влияние тяжести наказания на ожидаемую полезность становится больше, чем выгода от КА. Таким образом, вероятность разоблачения нарушителя ρ_n напрямую влияет на ожидаемую полезность от КА, в то время как выгода нарушителя W_m влияет опосредовано.

Анализ формулы $W_m = W_{mpj} - C_j$ позволяет сделать вывод, что стоимость реализации КА влияет на ожидаемую полезность. Если стоимость реализации КА больше выручки нарушителя в случае успешной реализации КА $W_{mpj} < C_j$, то выгоду нарушитель от реализации КА не получает .

2.2.3. Вероятность достаточности ожидаемой полезности

Для расчета достаточности ожидаемой полезности КА вида «А» с точки зрения нарушителя, при оценивании которой учитывается возможность проведения незаметной КА, необходимо определить вероятность достаточности ожидаемой полезности КА вида «*A*» с точки зрения нарушителя:

$$P(EUA) = \frac{EU_A}{EU_\Sigma}, \tag{2.12}$$

где

EU_A – ожидаемая полезность КА вида «А» с точки зрения нарушителя;

$EU_\Sigma = \sum_{j=1}^{J} EU_j$ – ожидаемая полезность с учетом всех доходов нарушителя,

j – порядковый номер метода КА, использованного нарушителем.

Анализ формулы (2.12) показал, что без ограничения общности в формуле (2.3) можно принято параметры *a*, *b* следующие значения: *b*=1, *a*=МРОТ (так как это та сумма, которую гражданин получит в любом случае, в качестве пособия по безработице).

2.2.4. Обоснование выбора источников первичной информации для расчета ожидаемой полезности от киберпреступления

При расчете вероятности проведения незаметной КА следует учитывать, что при оценке целесообразности проведения КА нарушитель, в первую очередь, опирается на свои знания, и, следовательно, на открытые источники информации о правонарушениях. В этой связи для расчета вероятности проведения незаметной КА можно использовать результаты анализа статей новостного агрегатора о

количестве громких судебных дел [105], а также статистику Генпрокуратуры РФ [104] о количестве зарегистрированных преступлений и данные ФинЦЕРТ [106, 107] о блокировке фишинговых ресурсов и телефонных номеров. Следовательно, в качестве оценки вероятности проведения незаметной КА можно использовать величину, вычисляемую по формуле:

$$\rho_m = \frac{A_m - A_{mf}}{A_m}, \tag{2.13}$$

где A_m – количество выявленных КА данного типа, A_{mf} – количество выявленных КА, закончившихся обращением в правоохранительные органы и/или арестом (наказанием преступника).

Отметим, что при оценке рисков международные стандарты рекомендуют учитывать ценность активов организации [13]. Однако нарушитель, в отличие от сотрудников организации, не знает их реальной ценности, поэтому он может оперировать только предполагаемой величиной и потенциальной величиной выгоды, которую может получить (например, за расшифровку данных после КА с помощью шифровальщика). Следовательно, потерянная ценность актива для организации в ходе успешной КА нарушителем не равна выгоде, получаемой нарушителем.

В этой связи в качестве оценки W_{mpj} можно использовать среднюю выручку нарушителя от рассматриваемого типа КА, которую можно вычислить на основе использования доступных статистических данных о КА. В качестве примера, рассчитаем средние значения выручки за 2017–2020 гг. для кредитно-финансового сектора (КФС) от наиболее распространенных типов КА. (Расчеты для других отраслей и типов КА можно провести аналогичным образом.)

Таблица 2-1. Данные по средней выручк и от успешной КА, проведенной на организацию

Период	Сектор экономики	Тип КА	Средняя выручка нарушителя от одной КА рассматриваемого типа, тыс. руб.	Кол-во КА рассматриваемого типа, шт.
2017	КФС	Целевые КА	49 034 [106, 107, 108]	39
2018	КФС	Целевые КА	3 824 [106, 107, 108]	72

2016, 2017, 2018	все	Нецелевые (спам-атаки, шифровальщики)	15,7 [109, 110]	200 000
2014	КФС	Нецелевые КА на клиентов КФС с использованием мобильного банкинга, транзакций с картами	11,6 [111]	300 000
2018	КФС	Нецелевые КА на физических лиц клиентов КФС с использованием мобильного банкинга, транзакций с картами	11,0 [105]	520 000
2019	КФС	Нецелевые КА на физических лиц клиентов КФС с использованием мобильного банкинга, транзакций с картами	11,1 [112, 113]	577 000
2019	КФС	Нецелевые КА на юридических лиц клиентов КФС с использованием мобильного банкинга, транзакций с картами	152 [112]	136 000
Первое полугодие 2020	КФС	Нецелевые КА на клиентов с использованием социальной инженерии	11,1 [114]	720 000

Компьютерные преступления, в отличие от других правонарушений, требуют от нарушителя наличия специальных навыков, знания методов и наличия возможности совершить КА. Следовательно, наибольшую выгоду от законной деятельности нарушитель получит, работая в сфере ИТ и ИБ, поэтому в качестве оценки W_i может быть принята средняя зарплата в сфере ИТ и ИБ, информация о которой, например, размещена сайте *Superjob* [115] (см. рисунок 2.1).

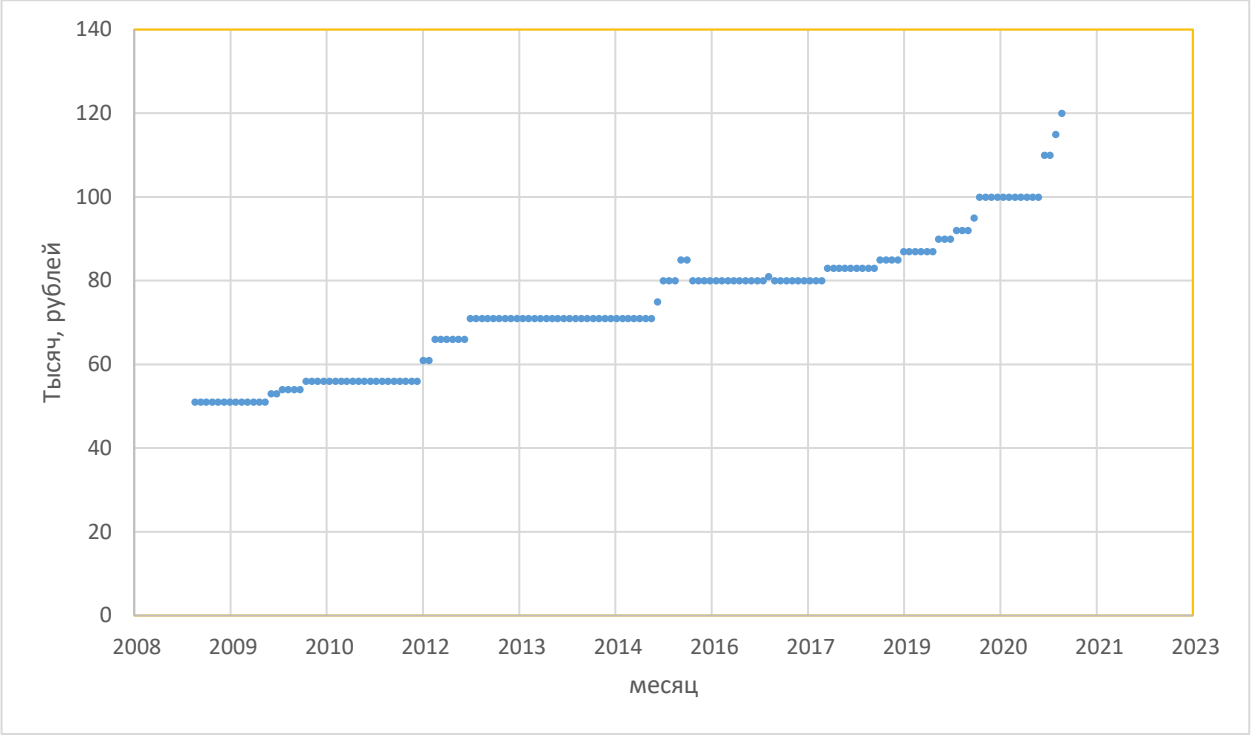

Рисунок 2-1. Средняя зарплата в сфере ИТ и ИБ в период с 2008 по 2020 гг.

Из рисунка 2-1 видно, что заработная плата в сфере ИБ с течением времени увеличивается. Принимая во внимание, что увеличение заработной платы прямо пропорционально компетентности потенциального нарушителя, можно предположить, с течением времени также будет увеличиваться эффективность проводимых им КА. Таким образом, при выборе функциональной зависимости дохода от времени, можно предположить, что функциональные зависимости $W_m(t)$ и $W_j(t)$ будут подобными друг другу, что подтверждают данные, представленные в таблице 2-1.

В связи с тем, что при проведении целенаправленных КА возможны отклонения от принятой гипотезы, обусловленные зависимостью ожидаемой полезности от тяжести и вероятности наказания, рассмотрим доступную статистику уголовных дел в области ИБ.

За совершение КА в Уголовном кодексе РФ предусмотрены штрафы за совершение КА, а также лишение свобод [116]. В этой связи при расчете тяжести наказания в денежном эквиваленте следует учитывать, как величину штрафа, так и величину потерь за период времени отбывания наказания. Потери, связанные с отбыванием наказания, можно рассчитывать, как потерю легального и

нелегального заработка за срок заключения. Детальные расчеты тяжести наказания за КА приведены в приложении Е, а краткие данные в таблице 2-2.

Таблица 2-2. Расчет тяжести наказания за проведение КА

Статья/пункт Уголовного кодекса РФ	Тяжесть наказания в терминах ожидаемой полезности
Статья 272. Неправомерный доступ к компьютерной информации	
п.1	$F = 24 \cdot (W_i + W_m)$
п.2	$F = 48 \cdot (W_i + W_m)$
п.3	$F = 60 \cdot (W_i + W_m)$
п.4	$F = 84 \cdot (W_i + W_m)$
Статья 273. Создание, использование и распространение вредоносных компьютерных программ	
п.1	$F = 66 \cdot (W_i + W_m)$
п.2	$F = 108 \cdot (W_i + W_m)$
п.3	$F = 84 \cdot (W_i + W_m)$
Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей	
п.1	$F = 24 \cdot (W_i + W_m)$
п.2	$F = 60 \cdot (W_i + W_m)$
Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации	
п.1	$F = 96 \cdot (W_i + W_m)$
п.2	$F = 108 \cdot (W_i + W_m)$
п.3	$F = 108 \cdot (W_i + W_m)$
п.4	$F = 132 \cdot (W_i + W_m)$
п.5	$F = 180 \cdot (W_i + W_m)$

Из таблицы 2.2 видно, что тяжесть наказания существенно превышает W_m. Следовательно, с точки зрения ожидаемой полезности при текущем уровне наказания нарушитель должен стремиться существенно снизить вероятность разоблачения ρ_n. Это подтверждается снижением средней суммы от целенаправленных КА в 2018 г. после серии уголовных дел возбужденных в отношении организаторов КА [105]. При этом необходимо отметить, что сумма выручки от успешно проведенной КА, с нашей точки зрения, является

заниженной, так как далеко не все пострадавшие организации обращаются в правоохранительные органы, или количество обращений очень мало. Высказанная точка зрения подтверждается далее примером, рассматриваемом в разделе 2.2.5.

2.2.5. Пример оценивания вероятности принятия решения преступником о проведении компьютерной атаки

Вычислим вероятности принятия решения преступником о проведении КА на примере КА, реализованной с помощью ВПО *Petya* [110, 117-120]. Типичная стоимость расшифровки файлов для одной организации, подвергшейся успешной обсуждаемой КА, составила («требует выкуп в размере $300 в биткоинах») $W_m = 18000$ руб. [118], при курсе 60 руб. за доллар в 2017 г. Таким образом, возможный ежемесячный заработок потенциального нарушителя составлял в 2017 г. $W_i = 80000$ руб. В то время как, в соответствии с п. 3 Статьи 273 законодательства РФ тяжесть наказания равнялась $F = 84 \cdot (W_i + W_m) = 84 \cdot 98000 = 8232000$ руб.

Оценим вероятность проведения незаметной КА, на основе анализа аналогичных КА за прошлые периоды. КА ВПО *Petya* предваряла широкомасштабная КА ВПО *WannaCry*, в которой использовалась аналогичную уязвимость ИБ. При этом организаторы КА ВПО *WannaCry* не были пойманы и наказаны, следовательно, $\rho_n = 0$. Суммарный заработок нарушителей от КА ВПО *WannaCry* составил 2,52 млн. руб. Учтем, что стоимость КА составляет 46,2 тыс. руб., определенная в соответствии с приложением F.

Так как в 2016 г. МРОТ составлял 6240 руб. [121], будем полагать, что в (2.3) $a = 6240, b = 1$.

Воспользовавшись (2.2), получаем:

$$EU = (1-\rho_n)U(W_m + W_i) + \rho_n U(W_m + W_i - F)$$
$$= (1-0)\cdot \ln\left(\frac{2520000 - 46200 + 80000 + 6240}{6240}\right) -$$
$$0\cdot \ln\left(83\cdot\left(\frac{2520000 - 46200 + 80000 + 6240}{6240}\right)\right) = 6,02.$$

В доступном описании сценария КА ВПО *Petya* на ИС, расположенные на территории Украины [118, 119], в том числе сообщается.

«Заражение вирусом началось через распространение обновления для ПО *M.E.Doc* 27 июня 2017 г. ПО *M.E.Doc* широко используется для подачи бухгалтерской отчетности на Украине, по данным специалистов ИБ, у фирмы на момент заражения было около 400 тысяч клиентов, что составляет порядка 90 % всех организаций страны» [118]. Таким образом, об КА стало известно только 27.06.2017, а именно от организаций Украины с 27.06.2017 по 28.06.2017: «в Департамент киберполиции Украины поступило более 1000 сообщений о вмешательстве в работу компьютерных сетей, что привело к сбоям в их работе. Из них официально с заявлениями в полицию обратились 43 компании» [118, 119].

Полный перечень мероприятий по защите от этой КА был разработан в течение суток после обнаружения КА [119]. «28 июня 2017 г. Кабинет Министров Украины сообщил, что масштабная КА на корпоративные сети и сети органов власти была остановлена. 4 июля 2017 г. с целью немедленного прекращения распространения червя *Petya* принято решение о проведении обысков и изъятии программного и аппаратного обеспечения компании, с помощью которого распространялось ВПО. Обыски проведены представителями Департамента киберполиции, следователями и при участии Службы безопасности Украины. Изъяты рабочие компьютеры персонала и серверное оборудование, через которое распространялось ПО» [118, 119].

По данным [110, 120] нарушители заработали $W_m = 720$ тыс. руб. Найдем вероятность разоблачения нарушителя при КА ВПО *Petya*. $\rho_n = \frac{A_{mf}}{A_m}$, где A_m – количество выявленных КА данного типа составило 1000 сообщений [118, 119],

A_{mf} – количество обратившихся в правоохранительные органы равнялось 43 [118, 119]). Таким образом, $\rho_n = \frac{43}{1000} = 0,04$. В связи с тем, что вероятность разоблачения нарушителей оказалось достаточно низкой, далее было реализовано еще 2 аналогичных КА с использованием ВПО *NotPetya* и *BadRabbit*, однако, с меньшей прибылью.

Из таблиц 2-1 и 2-2 видно, что нецеленаправленные КА реализуются массово, как в примере с описанной выше КА, проведенной с использованием ВПО *Petya*, у которой $W_j >> W_m$. ($W_j = 80000, W_m = 720000$).

Таким образом, КА ВПО *Petya* проводилась в условиях, когда был обеспечен приемлемый уровень среднего заработка от одной КА, который, с одной стороны, позволял получить ожидаемую полезность от КА, и относительно небольшую вероятность разоблачения нарушителя, с другой стороны.

Отметим, что за последние 3 года было рассмотрено несколько громких уголовных дел, заведенных на группы нарушителей, совершивших целенаправленные КА [105], что привело к существенному уменьшению средней суммы прибыли нарушителя от единичной целенаправленной КА.

2.2.6. Анализ результатов

На основе теории принятия решений, общей практики выявления и предупреждения правонарушений, а также ИТ-подходов к выявлению уязвимостей предложена и обоснована математическая модель принятия решений нарушителем о проведении КА, описывающая связь между вероятностью КА и ключевыми факторами атаки.

Из проведенного анализа математической модели принятия решений нарушителем о проведении КА можно сделать следующие выводы:

1. Значение ожидаемой полезности, при прочих равных условиях, определяется, в первую очередь, вероятностью разоблачения нарушителя (вероятностью проведения незаметной КА) для нарушителя, склонного к риску, и

для нарушителя, не склонного к риску, тяжестью наказания. Следовательно, необходимо выстроить дифференцированную систему защиты ИБ в зависимости от типа нарушителя.

2. Можно ожидать, что увеличение доходов от легальной деятельности специалистов ИБ приведет к значительному сокращению числа нарушителей.

3. Количество КА за определенный период времени зависит от вероятности проведения незаметной КА, тяжести наказания, наличия и величины альтернативных доходов (выгод).

4. Осуществление защиты от КА возможно за счет изменения восприятия преступником возможностей (в том числе, соотношения между выгодой и потерями) совершения преступления;

5. Необходимо разрабатывать дифференцированные системы ИБ, уменьшающие вероятности наиболее опасных для данной ИС КА, которые будут являться для нарушителей, адекватно оценивающих риски, возникающие вследствие проводимой КА, и учитывающих тяжесть наказания за совершаемое им деяние, предусмотренное действующим законодательством РФ, сдерживающим фактором.

6. Нарушитель, безнаказанно совершивший результативную КА, продолжит в будущем предпринимать попытки реализации компьютерных атак.

7. Количество КА за определенный период времени зависит от вероятности того, что КА окажется незамеченной, тяжести наказания, наличия и величины альтернативных доходов (выгод) у нарушителя.

8. Можно ожидать, что увеличение доходов от легальной деятельности специалистов ИБ существенно сократит количество нарушителей.

2.3. Разработка математической модели, описывающей динамику возможности реализации компьютерной атаки во времени

В предыдущем разделе была построена математическая модель условной вероятности достаточности ожидаемой полезности КА с точки зрения нарушителя, основанная на учете условий принятие решения о проведении КА,

наличие (ожидаемое появление) мер защиты от данного метода КА. Для разработки математической модели, описывающей динамику возможности реализации КА во времени, проведем анализ особенностей КА с точки зрения нарушителя (этапы и методы реализации КА) и факторов, определяющих динамику изменения возможности реализации КА.

При этом учтем, что компьютерные преступления, в отличие от правонарушений, являющихся предметом, изучаемым криминологией, требуют от нарушителя наличия специальных знаний, умений и навыков, а также возможности практически совершить КА. Рассмотрим подробнее умения и навыки нарушителя. Знания о методах КА нарушитель может приобрести в *DarkNet* – области интернета, в которые не может попасть обычный пользователь через поисковики *Google* или *Yandex*. Для доступа к *DarkNet* необходимо использовать ПО обеспечивающее анонимное подключение, например, *The Onion Router (TOR)*. Для большей конфиденциальности нарушители на форумах *DarkNet* используют технологию *Virtual Private Network (VPN)*. Анализ форумов в *DarkNet* позволяет собрать информацию о стратегиях, тактиках и методах, которые используют и/или разрабатывают нарушители для реализации КА. Различные решения по сбору информации с форумов *DarkNet* рассматриваются в [32-35, 122].

Таким образом, на подготовительном этапе проведения КА нарушитель стремится получить сведения о новых для него технологиях проведения КА, которые, следуя [48], является синонимом понятия «инновация» (инновация – технологическая идея, метод или объект, являющийся новым для члена социальной системы). В этой связи, можно предположить, что динамика КА может быть построена на основе положений и математических моделей ТДИ (здесь диффузия инноваций – это процесс, с помощью которого инновации распространяются по каналам передачи с течением времени среди членов социальной системы), развитой в Э. Роджерсом [48], Ф. Бассом [49], Э. Мэнсфилдом [50] и Т. Хагерстранда [51].

Для подтверждения высказанной выше гипотезы, рассмотрим базовые понятия ТДИ [48]:

1. Инновация – технологическая идея, метод или объект, являющийся новым для члена социальной системы.

2. Канал передачи – процесс передачи информации от одного члена социальной системы одному или нескольким членам социальной системы, основной принцип функционирования которого основан на предположении о том, что передача инновации наиболее часто происходит между похожими индивидуумами.

3. Время – характеризует динамику распространения инновации.

4. Социальная система – сеть взаимосвязанных элементов, занятых решением данной задачи. (В связи с тем, что элементы социальной системы не идентичны в своем поведении, в ТДИ отдельно выделена социальная система с шаблонным поведением элементов, например, государственная или военная структура). Динамика процесса диффузии инноваций определяется вероятностью взаимодействия данного элемента с любым другим элементом, которая не зависит от похожести ее элементов.

Напомним, что модель Басса базируется на предположении о том, что вероятность совершения покупки данной технологии в момент времени T покупателями, ранее не совершивших данную покупку, $P(T)$ является линейной функцией числа покупателей, совершивших покупку данной технологии за время $0 \le t < T$ [49], $Y(T)$:

$$P(T) = p + \frac{q}{m} Y(T), \tag{2.14}$$

здесь:

$Y(0) = 0,$

p – константа – вероятность покупки инновации в момент времени $T = 0,$ называемая коэффициентом инновации;

q – константа, называемая, коэффициентом имитации;

m – потенциал рынка (число участников рынка);

$\frac{q}{m}Y(T)$ – приращение вероятности совершения покупки под влиянием информации о числе покупателей, совершивших покупку данной технологии за время $0 \le t < T$.

Отметим, что здесь время *T* является безразмерной величиной, измеряемой в долях выбранной единицы измерения времени, например, месяца. Тогда значение временного интервала длительностью 1 день принимается равным 1/30, соответственно, значение интервала равного 1 год принимается равным 12.

Вероятность покупки технологии в момент времени *T* вычисляется по формуле [49]:

$$f(T)/\big(1-F(T)\big) = P(T) = p + \frac{q}{m}Y(T) = p + qF(T), \qquad (2.15)$$

где

$f(T)$ – вероятность покупки технологии в момент времени *T*;

$$F(t) = \int_0^T f(t)\,dt.$$

Из (2.15) видно, что

$$Y(T) = \int_0^T S(t)\,dt = m\int_0^T f(t)\,dt = mF(T), \qquad (2.16)$$

где $S(T)$ – количество технологий, приобретенных в момент времени *T*. Подставляя (2.16) в (2.16), получаем

$$S(T) = m\,f(T) = P(T)\big(m - Y(T)\big) = \left(p + \frac{q}{m}\int_0^T S(t)\,dt\right)\left(m - \int_0^T S(t)\,dt\right) = \qquad (2.17)$$
$$pm + (q-p)Y(T) - \frac{q}{m}Y^2(T).$$

Так как

$$f(T) = \big(p + qF(T)\big)\big(1 - F(T)\big) = p + (q-p)F(T) - qF^2(T),$$

а $f(T) = \frac{dF(T)}{dT}$, получаем следующее дифференциальное уравнение:

$$dT = \frac{dF}{p + (q - p)F - qF^2}, \tag{2.18}$$

общее решение которого имеет вид:

$$F = \frac{q - pe^{-(T+C)(p+q)}}{q\left(1 + e^{-(T+C)(p+q)}\right)}, \tag{2.19}$$

где C – постоянная, значение которой находится из начальных условий.

Так как $F(0) = 0,$ из (2.19) находим

$$C = -\frac{\ln(p/q)}{p+q}. \tag{2.20}$$

Подставляя далее (2.20) в (2.19), находим искомое решение (2.18):

$$F(T) = \frac{1 - e^{-(p+q)T}}{(q/p)e^{-(p+q)T} + 1},$$

соответственно,

$$f(T) = \frac{(p+q)^2}{q} \frac{e^{-(p+q)T}}{\left((q/p)e^{-(p+q)T} + 1\right)^2},$$

$$S(T) = \frac{m(p+q)^2}{q} \frac{e^{-(p+q)T}}{\left((q/p)e^{-(p+q)T} + 1\right)^2}.$$

Типичные зависимости $S(T)$, $Y(t)$ при $q < p$ и $q > p$ представлены на рисунках 2.2–2.5, соответственно.

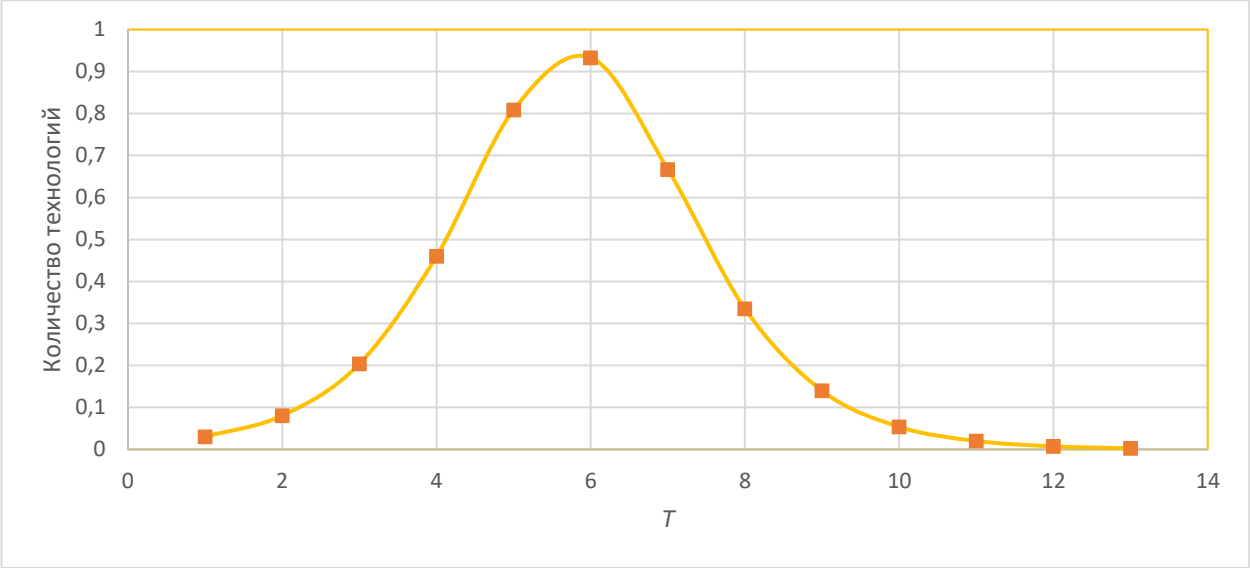

Рисунок 2-2. Зависимость $S(T)$, $q=1$, $p=0,003$

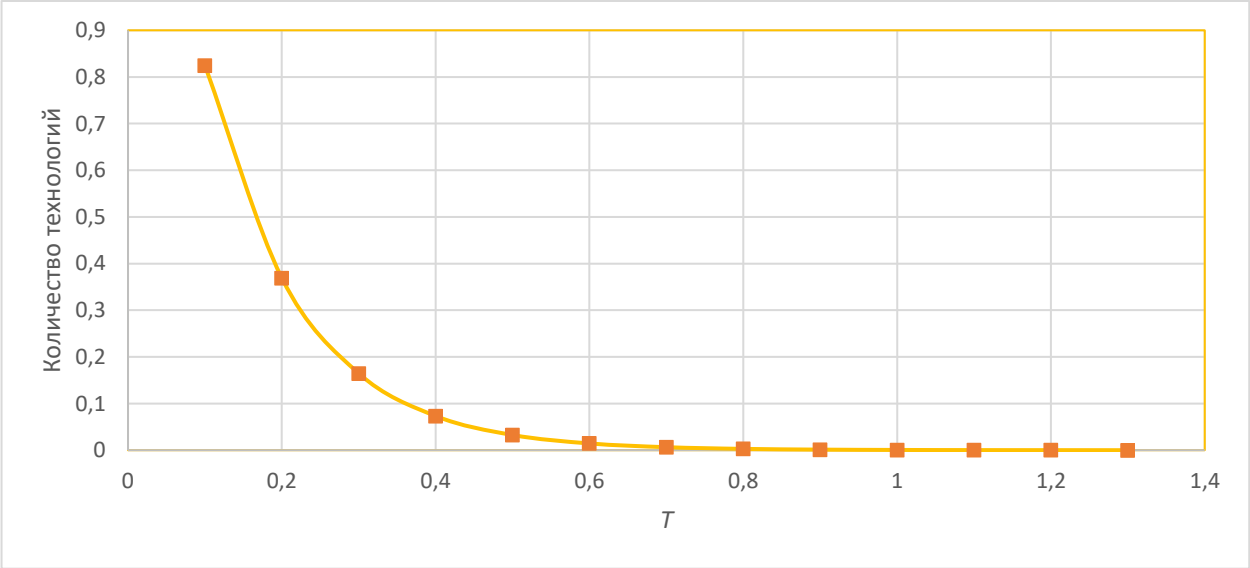

Рисунок 2-3. Зависимость $S(T)$, $q=0,1$, $p=8$

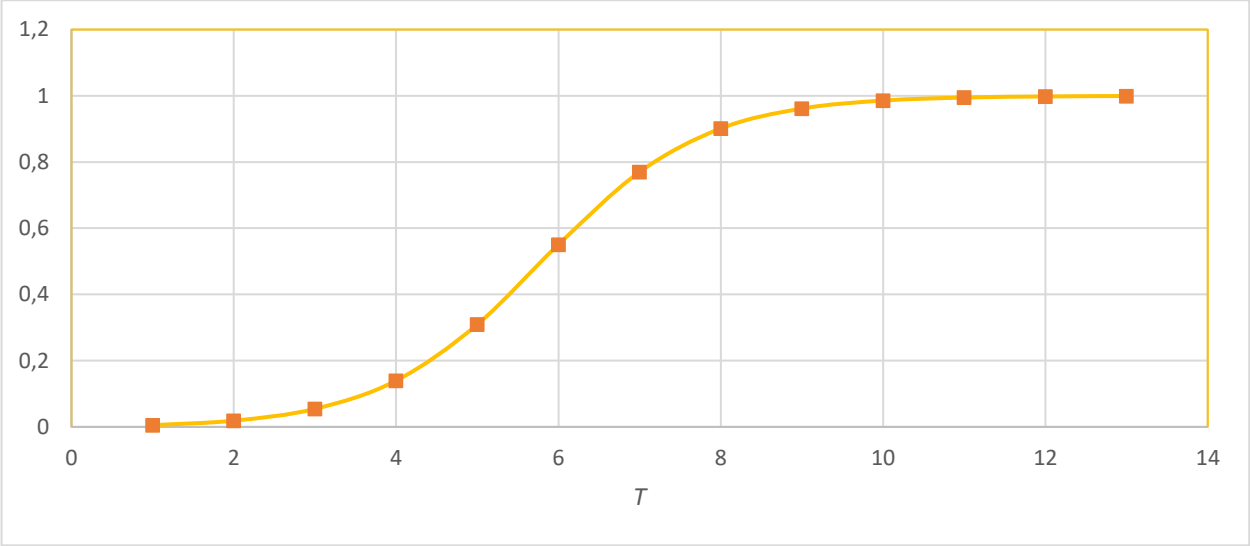

Рисунок 2-4. Зависимость $Y(T)$, $q=1$, $p=0,003$

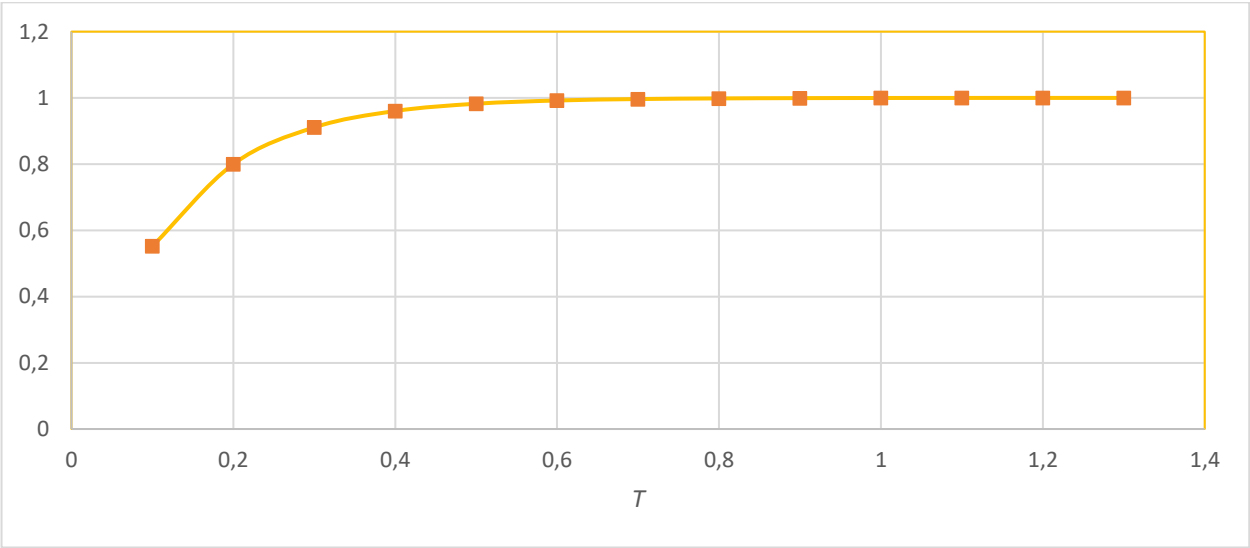

Рисунок 2-5. Зависимость $Y(T)$, $q=0,1$, $p=8$

Из рисунков 2.2, 2.3 видно, что при $q<p$ зависимость $S(T)$ является монотонно убывающей, при $q>p$ – функция $S(T)$ на интервале $[0,T^*]$,

где

$$T^*=-\frac{1}{p+q}\ln\left(\frac{p}{q}\right)=\frac{1}{p+q}\ln\left(\frac{q}{p}\right),$$

монотонно возрастает, достигая своего максимального значения $S(T^*)=S^*$,

$$S^*=\frac{m(p+q)^2}{4q},$$

соответственно,

$$Y\left(T^*\right)=\int_0^{T^*} S\left(t\right)dt=\frac{m\left(q-p\right)}{2q},$$

и далее монотонно убывает.

В связи с тем, что динамика диффузии инноваций также описывается в дискретном времени приведем дискретный аналог (2.17) [49]:

$$S_T=a+bY_{T-1}+cY_{T-1}^2,$$

где $T=2,3,\ldots,$ $Y_{T-1}=\sum_{t=1}^{T-1}S_t,$ коэффициенты $a,$ $b,$ c являются аналогами коэффициентов $pm,$ $q-p,$ $-q/m$ соответственно, в (2.17).

Из рисунков 2.4, 2.5, видно, что зависимости $Y\left(t\right)$, описывающие накопленные суммы приобретенных инноваций от времени, описываются значимостями вида:

$$Y(t)=\frac{1}{1+\alpha e^{-\beta t}}, \tag{2.21}$$

где α,β – параметры модели, называемых *s*-образными кривыми Перла-Рида.

Согласно исследованиям, проведенным [51] инновация может также развиваться по каскадной модели, описываемой следующе формулой:

$$Y(t)=\begin{cases}\dfrac{1}{1+\alpha_1 e^{-\beta_1(t-t_0)}}, \text{ если } t_0\le t\le t_1,\\ \dfrac{1}{1+\alpha_1 e^{-\beta_1(t_1-t_0)}}+\dfrac{1}{1+\alpha_2 e^{-\beta_2(t-t_1)}}, \text{ если } t_1<t\le t_2,\\ \cdots\\ \dfrac{1}{1+\alpha_1 e^{-\beta_1(t_1-t_0)}}+\dfrac{1}{1+\alpha_2 e^{-\beta_2(t_2-t_1)}}+\cdots+\dfrac{1}{1+\alpha_n e^{-\beta_n(t-t_{n-1})}}, \text{ если } t_{n-1}<t\le t_n,\end{cases} \tag{2.22}$$

где

$\left[t_0,t_1\right]$ – длительность первого этапа развития инновации;

$\left]t_1,t_2\right]$ – длительность второго этапа развития инновации;

…

$]t_{n-1}, t_n]$ – длительность *n*-го этапа внедрения инновации.

Напомним, что скорость изменения диффузии инновации по Э. Роджерсу [48] зависит от пяти основных свойств инновации, по которым потенциальные потребители принимают решение об использовании или неиспользовании инновации.

1. Относительные преимущества инновации (*relative advantage*) – степень превосходства перед другими (зачастую аналогичными) инновациями, выражающиеся в экономических или социальных категориях (прибыльность, экономичность, удобство и удовлетворенность).

2. Совместимость (*compatibility*) инновации – степень соответствия инновации существующим требованиям, прошлому опыту и потребностям члена социальной системы.

3. Сложность (*complexity*) инновации – степень сложности для понимания и использования; предполагается, что сложность инновации негативно связана с ее восприятием.

4. Простота апробации (*trialability*) инновации – возможность апробации инновации в ограниченных масштабах (в ряде случаев данную характеристику инновации отождествляют с этапностью, делимостью инновации (*divisibility*) на отдельные части).

5. Коммуникативность (*communicability*) инновации – видимость результатов использования инновация между другими членами социальной системы.

В основе модели [48] лежит деление покупателей по признаку индивидуальной предрасположенности к восприятию инновации:

- новаторы (*innovators*, 2,5%);
- ранние последователи (*early adopters*, 13,5%);
- раннее большинство (*early majority*, 34%);
- позднее большинство (*late majority*, 34%);
- опоздавшие (*laggards*, 16%).

Корректность такого упрощения для новых прогрессивных технологий, к которым относятся ИТ и ИБ технологии, была подтверждена Э. Мэнсфилдом [50].

Из приведенного выше описания базовых понятий ТДИ, понятно, что аналогом понятия «инновации» в терминах КА является новый метод КА, понятия «канал передачи» – форумы и чаты *DarkNet*, понятия «социальная система» – нарушители, общающиеся в сети *DarkNet*. Следовательно, динамику информации о конкретном методе КА, распространяемом/обсуждаемом в *DarkNet*, можно описать с точки зрения ТДИ.

В терминах КА диффузия – это процесс, с помощью которого информация о данном методе реализации КА распространяется по каналам передачи с течением времени среди нарушителей.

В терминах КА процесс принятия решения о возможности использования данного метода КА проходит пять этапов:

1. Знание – нарушитель (или другое устройство по принятию решений) узнает об методе КА и понимает, как он реализуется.

2. Убеждение – нарушитель формирует представление о преимуществах и недостатках метода КА.

3. Принятие решения – нарушитель принимает решение о применимости данного метода КА (принимает или не принимает к использованию).

4. Применение – нарушитель использует выбранный метод КА. На этом этапе осуществляется адаптация (проверка) выбранного метода КА.

5. Подтверждение – нарушитель принимает решение о дальнейшем использовании выбранного метода КА.

Таким образом, возможность реализации КА зависит как от знаний и умений нарушителя – (три первых этапа), так и от практической возможности реализовать КА в инфраструктуре организации, являющейся объектом КА (четвертый и пятый этапы). В этой связи «социальная система» – есть «узлы» организации, на которые воздействует нарушитель для распространения КА. При этом «каналы», обеспечивают взаимосвязи «узлов» организации между собой и внешней

инфраструктурой, через которую нарушитель получает доступ. Действительно, ключевое правило ТДИ вероятность взаимодействия (заражения КА) «узла» с любым другим «узлом» организации одинакова, она не зависит от похожести элементов. Следовательно, если в организации внедрены средства ЗИ от используемого метода КА, то распространение КА происходить не будет. Следовательно, динамику распространения метода КА от «узла» к «узлу» организации в ходе ее реализации можно описать с точки зрения ТДИ, считая:

$F(t)$ – суммарным количеством нарушителей в *DarkNet*, выбравших новый метод КА к моменту t (в терминах реализации КА – суммарное количество нарушителей, использующих рассматриваемый метод КА к моменту t);

t – безразмерной величиной, определяемой по формуле $t = \frac{T - T_0}{месяц}$,

здесь T – время, T_0 – время начала распространения метода КА, шаг распространения КА – месяц;

m – потенциалом рынка (количество потенциальных нарушителей);

$m - F(t)$ – количеством пользователей *DarkNet*, не использующих рассматриваемый метод КА;

p – коэффициентом инновации, т.е. коэффициент, характеризующим внешнее воздействие на нарушителей в *DarkNet* с целью приобретения/использования рассматриваемого метода КА (в терминах реализации КА – коэффициент, характеризующий внешнее воздействие нарушителя на «узел» с помощью КА);

q – коэффициентом имитации, т.е. – коэффициентом, характеризующим межличностное взаимодействие нарушителей в *DarkNet*, которые уже приобрели/использовали данный метод КА (в терминах реализации КА – коэффициент, характеризующий внутреннее взаимодействие «узлов», т.е. передача КА от «узла» к «узлу»).

Также необходимо отметить, что новые методы КА зачастую используют доработанные старые методы, следовательно, можно ожидать, что зависимость

числа атакованных узлов от времени с течением времени будет описываться каскадной моделью (2.22).

Возможность рассмотрения «узлов» наиболее вероятного взлома ИС, позволяет улучшить качество прогноза, используемого для выявления новых уязвимостей ПО и оценок векторов КА. Подтверждением возможности и эффективности применения такого подхода являются результаты [44], где продемонстрировано, что ограничение области анализа уязвимостей ИБ поиском только уязвимых частей программного кода (например, элементов взаимодействия с внешними системами, пользовательских интерфейсов) позволяет улучшить качество прогнозирования новых уязвимостей. Таким образом, рассмотрение «узлов» наиболее вероятного взлома ИС, позволяет улучшить качество прогноза, используемого для выявления новых уязвимостей ПО и оценок векторов КА.

Для подтверждения адекватности описанных в данном разделе математических моделей, описывающих динамику развития КА, были проведены:

– анализ доступных данных о динамике КА, реализованной с помощью ВПО *WannaCry*;

– анализ доступных данных о появлении новых видов ВПО;

– экспериментальные исследования, результаты которых обсуждаются далее.

2.4. Подтверждение адекватности математической модели динамики распространение компьютерной атака на примере компьютерной атаки, реализованной с помощью вредоносного программного обеспечения *WannaCry*

В разделе 2.3 определена аналогия «социальной системы» как совокупности «узлов» организации, на которые воздействует нарушитель для распространения КА. Таким образом, динамика изменения вероятности КА эквивалентна динамике увеличения количества «зараженных» узлов, характеризующейся отношением

числа узлов, зараженных в результате успешно реализованной КА, к общему количеству узлов, которое далее будем называть относительным числом атакованных узлов КС в момент времени *t*.

2.4.1. Динамика реализации КА

Для анализа динамики распостранения КА, характеризующейся зависимостью относительного числа атакованных узлов КС от времени были использованы соответствующие данные, зарегистрированные во время проведения КА с помощью ВПО *WannaCry*, которые размещены на сайте *MalwareTech* [123]. Исходная информация представляет собой отсчеты числа атакованных узлов за выбранный период времени (1 минуту, 5 минут, 30 минут, 1 час, 24 часа) от времени, представленные в виде графика (см. рисунок 2-6). Из рисунка 2–6 видно, что при наведении курсора мыши на соответствующую точку графика появялется окно, в котором отображается информация о дате, времени (здесь 00:00 часов соответствует 24:00 по шкале измерения времени, используемой в РФ) и числе зараженных узлов (New). Однако возможности выгрузить первичную информацию в виде файла разработчик сайта не предоставил. В результате пришлось извлекать ее вручную, последовательно просматривая каждую точку зависимости числа вновь атакованных в течение 24 часов узлов от времени. Полученная первичная информация представлена в таблице 2–3, из которой видно, 02.06.2017 информация о числе вновь зараженных узлов не выкладывалась на сайте, а с 03.06.2017 изменилась время публикации данных с 24:00 часов на 04:00.

Для нахожденния аппрокисмации зависимости числа вновь зараженных узлов КС от времени требуется преобразовать значения абсцисс отсчетов, задаваемых в формате дата/время, анализируемой зависимости в порядковую временную шкалу. Для выполения данной процедуры, как очевидно, необходимо выбрать единицу измерения времени (принимая во внимание отмеченные выше особенности первичных данных была выбрана единица измереннія 1 час) и далее

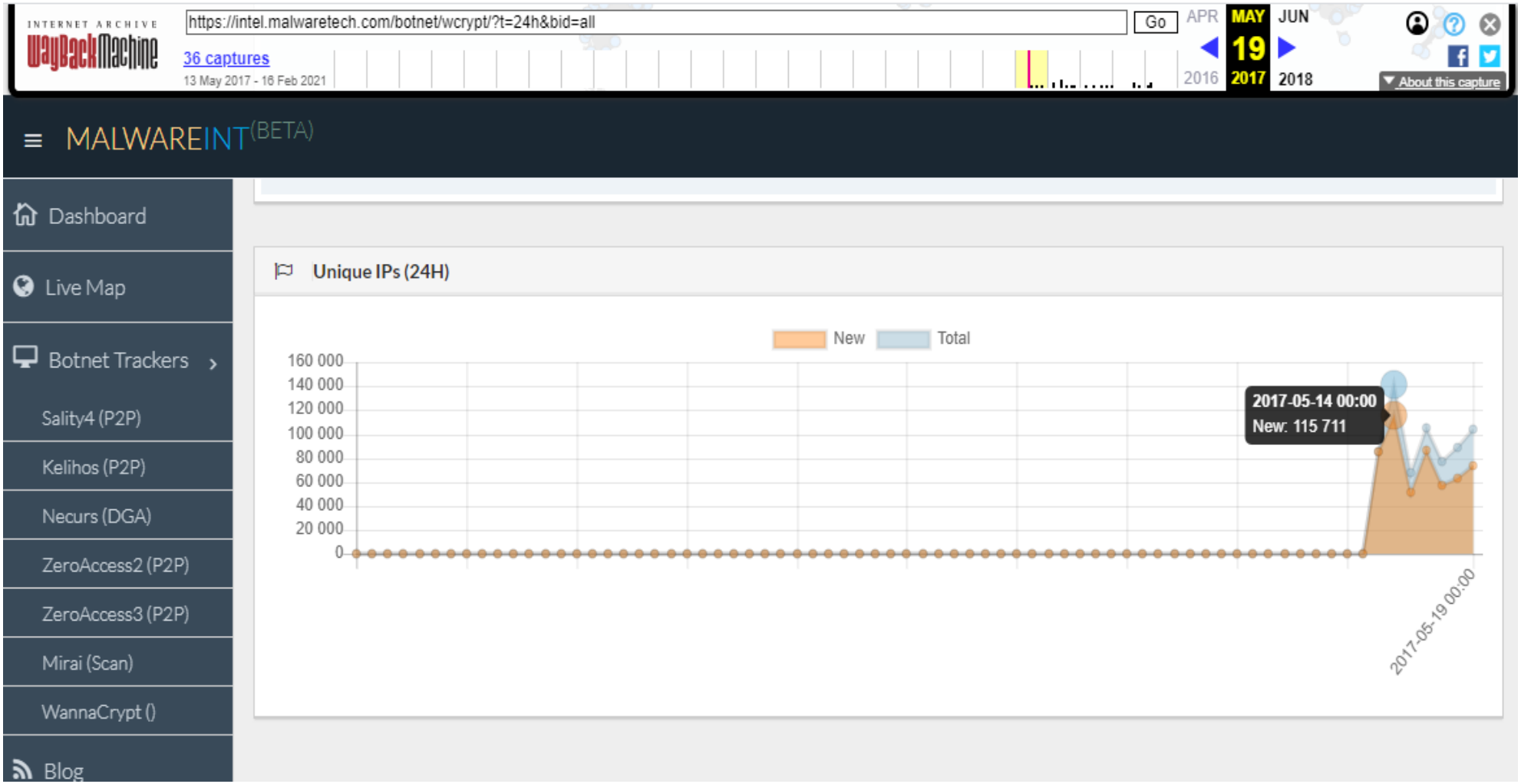

Рисунок 2-6. Фрагмент скриншота экранной формы сайта [123] в режиме обораження зависимости числа атакованных узлов в течение 24 часов от времени

Таблица 2-3. Первичная информация о зависимости числа зараженных в течение 24 часов узлов КС от времени

№	Дата/время	New	№	Дата/время	New	№	Дата/время	New	№	Дата/время	New
1	2017-05-11 00:00	0	23	2017-06-03 04:00	86988	45	2017-06-24 04:00	83312	67	2017-07-16 04:00	61126
2	2017-05-12 00:00	0	24	2017-06-04 04:00	76783	46	2017-06-25 04:00	73195	68	2017-07-17 04:00	61557
3	2017-05-13 00:00	85614	25	2017-06-05 04:00	86725	47	2017-06-26 04:00	67343	69	2017-07-18 04:00	70938
4	2017-05-14 00:00	115711	26	2017-06-06 04:00	89673	48	2017-06-27 04:00	72213	70	2017-07-19 04:00	70633
5	2017-05-15 00:00	67840	27	2017-06-07 04:00	83045	49	2017-06-28 04:00	67043	71	2017-07-20 04:00	68231
6	2017-05-16 00:00	86185	28	2017-06-08 04:00	71259	50	2017-06-29 04:00	61905	72	2017-07-21 04:00	67885
7	2017-05-16 00:00	57179	29	2017-06-09 04:00	88590	51	2017-06-30 04:00	61722	73	2017-07-22 04:00	67463
8	2017-05-18 00:00	63326	30	2017-06-10 04:00	83277	52	2017-07-01 04:00	73846	74	2017-07-23 04:00	60285
9	2017-05-19 00:00	73274	31	2017-06-11 04:00	77378	53	2017-07-02 04:00	75301	75	2017-07-24 04:00	61098
10	2017-05-20 00:00	63976	32	2017-06-12 04:00	77893	53	2017-07-03 04:00	73460	76	2017-07-25 04:00	69926
11	2017-05-21 00:00	57471	33	2017-06-13 04:00	81047	55	2017-07-04 04:00	78858	77	2017-07-26 04:00	67780
12	2017-05-22 00:00	62492	34	2017-06-14 04:00	82856	56	2017-07-05 04:00	79829	78	2017-07-27 04:00	67474
13	2017-05-23 00:00	44752	35	2017-06-15 04:00	80762	57	2017-06-06 04:00	76506	79	2017-07-28 04:00	69088
14	2017-05-24 00:00	83312	36	2017-06-16 04:00	81625	58	2017-07-07 04:00	77613	80	2017-07-29 04:00	67645
15	2017-05-25 00:00	84508	37	2017-06-17 04:00	62338	58	2017-07-08 04:00	72412	81	2017-07-30 04:00	65055
16	2017-05-26 00:00	71629	38	2017-06-18 04:00	43237	60	2017-07-09 04:00	70705	82	2017-07-31 04:00	65684
17	2017-05-27 00:00	95085	39	2017-06-19 04:00	12918	61	2017-07-10 04:00	71908	83	2017-08-01 04:00	71252
18	2017-05-28 00:00	83660	40	2017-06-20 04:00	52429	62	2017-07-11 04:00	75979	84	2017-08-02 04:00	68110
19	2017-05-29 00:00	82333	41	2017-06-21 04:00	83496	63	2017-07-12 04:00	75556	85	2017-08-03 04:00	51434
20	2017-05-30 00:00	92506	42	2017-06-22 04:00	80673	64	2017-07-13 04:00	72808	86	2017-08-04 04:00	114
21	2017-05-31 00:00	90628	43	2017-06-23 04:00	77079	65	2017-07-14 04:00	71428	87	2017-08-05 04:00	0
22	2017-06-01 00:00	32292	44	2017-06-24 04:00	75640	66	2017-07-15 04:00	68015	88	2017-08-05 04:00	0

и далее указать значение моментов времени между последовательными измерениями: первый отсчет – 0, второй отсчет 24 часа и т.д., в связи с отсутствием данных на 02.06.2017 момент времени между пердшествующим ему и данным отсчетом выбирался равным 52 часа. Тогда накопленная сумма значений временных интервалов между отсчетами анализируемой зависимости есть искомая временная сетка, значения узлов которой измеряются в часах. Для того, чтобы в анализируемой зависчимости присутсвовала информация, соответствующая периоду до начала КА и после ее окончания, данные, представленные в таблице *2-6*, дополнялись справа и слева 17-ю нулевыми отсчетами. Полученная в результате проведенных преобразований зависимость представлена на рисунке 2–7.

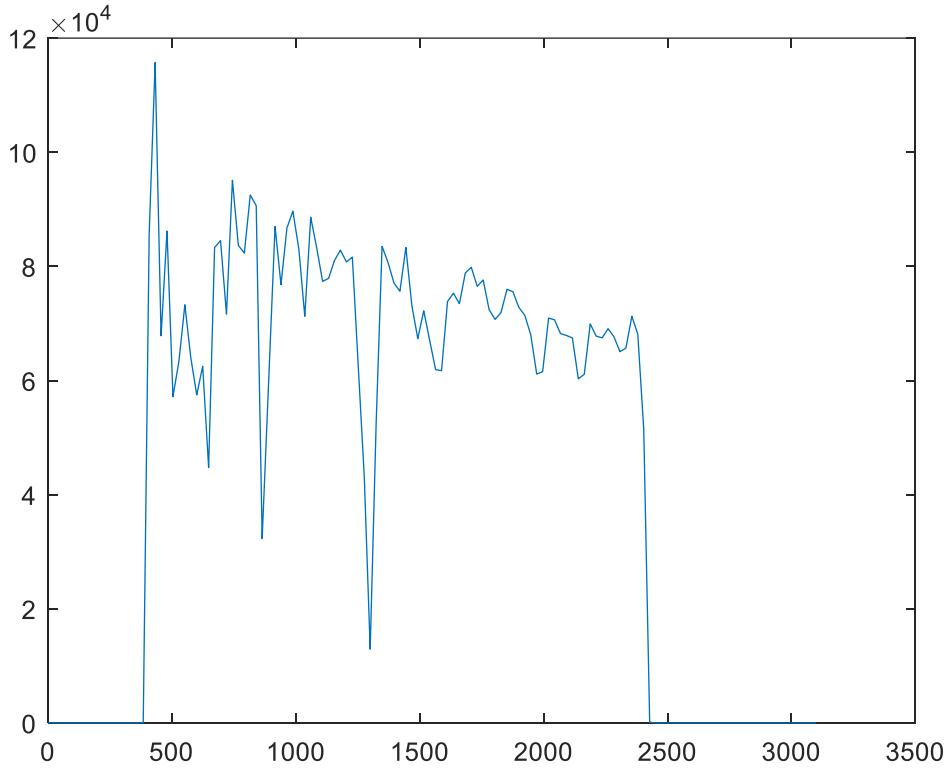

Рисунок 2-7. Зависимость числа вновь зараженных узлов КА ВПО WannaCry в период с 26.04.2017 по 31.08.2017

Далее для нахождения зависимости общего количества зараженных узлов в течение 24 часов от времени, вычислялись первые накопленные суммы зависимости, представленной на рисунке 2–7. Зависимость общего количества зараженных узлов в течение 24 часов ВПО *WannaCry* от времени, нормированная на максимальное число зараженных узлов, представлена на рисунке 2–8.

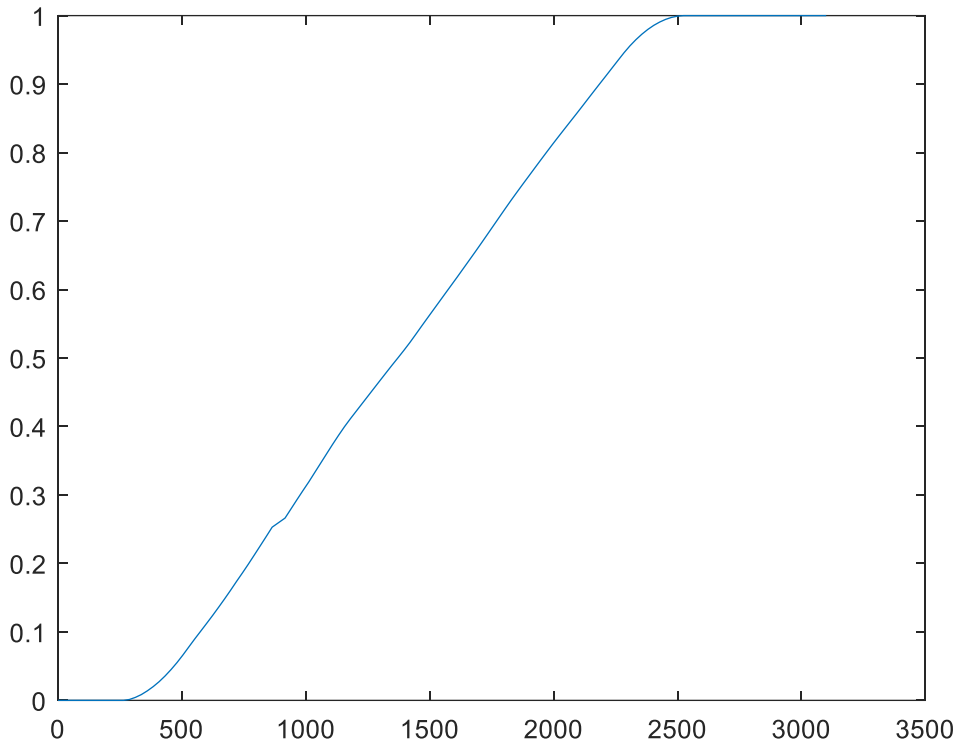

Рисунок 2-8. Зависимость числа вновь зараженных узлов КА ВПО WannaCry в период с 26.04.2017 по 31.08.2017

Визуальный анализ зависимости, представленной на рисунке 2–8 позволяет предположить, что данную зависимость можно аппроксиммировать *s*-образной кривой Перла-Рида (2.21). Результаты, подтверждающие данную гипотезу представлены в следующем разделе.

2.4.2. Математическое обоснование выбора апроксимирующей функции методом наименьших квадратов

Рассмотрим результаты аппроксимации зависимости, представленной на рисунке 2–8, в соответствие с методом наименьших квадратов с помощью линейной и квадратической функций, а также *s*-образной кривой Перла-Рида (2.21). Значения коэффициентов линейной и квадратической аппроксимирующих функций, а также *s*-образной кривой Перла-Рида (2.21), находились, соответственно, из условий:

$$\arg\min_{\alpha_1,\alpha_2}\left(\sum_{i=1}^{N}\left(y_i-\left(\alpha_1 t_i+\alpha_2\right)\right)\right)^2, \tag{2.23}$$

$$\arg\min_{\alpha_1,\alpha_2,\alpha_3}\left(\sum_{i=1}^{N}\left(y_i-\left(\alpha_1 t_i^2+\alpha_2 t_i+\alpha_3\right)\right)\right)^2, \tag{2.24}$$

$$\arg\min_{\alpha_1,\alpha_2,\alpha_3,\alpha_4}\left(\sum_{i=1}^{N}\left(y_i-\left(\alpha_1+\frac{\alpha_2}{1+\alpha_3\exp\left(-\left(\alpha_4\left(t_i-t_1\right)\right)\right)}\right)\right)\right)^2, \tag{2.25}$$

N – число отсчетов аппроксимируемой зависимости. Для нахождения решения задач (2.23), (2.24) использовалась функция пакета MATLAD regress.m, задачи (2.25) – функция fminsearch.m.

Значения коэффициентов аппроксиммирующих функций, а также остатки данных моделей представлены в таблице 2-4. Графики аппроксимируемой зависимости и аппроксимирующие функции представлены на рисунке 2–9.

Таблица 2-4. Значения коэффициентов аппроксимирующих функций

Тип функции	α_1	α_2	α_3	α_4	Дисперсия остатков модели
Линейная	0,00041	–0.073	–	–	0.065
Квадратическая	$-5\cdot10^{-8}$	0,00056	–0.15	–	0.053
s-образная	–0.11025	1.18080	0.00197	13.7642	0.021

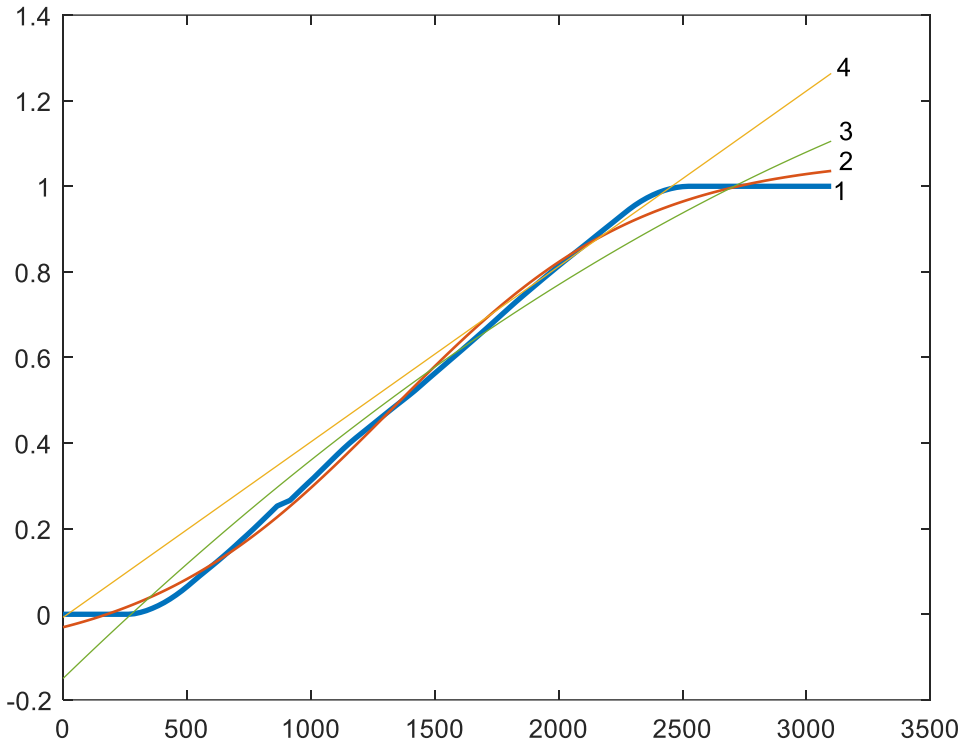

Рисунок 2-9. Аппроксимации зависимости общего числа зараженных узорв КС, зараженных ВПО WannaCry, от времени: 1 - аппроксимируемая зависимость; 2 - s-образная кривая Перла-Рида; 3 - квадратическая функция 4 - линейная функция

Из таблицы 2-4, что минимальное значение среднеквадратического отклонения остатков аппроксимации оказывается у s-образной кривой Перла-Рида, что подтверждает провомерность ее использования в дальнейшиxx исследованиях математической модели, описаной в разделе 2.3.

2.5. Экспериментальные исследования динамики развития компьютерной атаки

2.5.1. Описание экспериментального стенда

Для экспериментального подтверждения адекватности математических моделей, описывающих динамику развития КА был использован программно-аппаратный комплекс (ПАК) обучения методам обнаружения, анализа и

устранения последствий КА «*Ampire*» [125], разработанный компанией ОА «Перспективный мониторинг».

ПАК «*Ampire*» позволяет моделировать типовые и специализированные ИС, активировать векторы КА, характерные для внешнего и внутреннего нарушителей. Комплекс предоставляет пользователю специализированное ПО для обнаружения следов КА, а также инструменты для повышения уровня защищенности ИС, на которой проходит тренировка. Интерфейс ПАК «*Ampire*» представлен на рисунке 2-10.

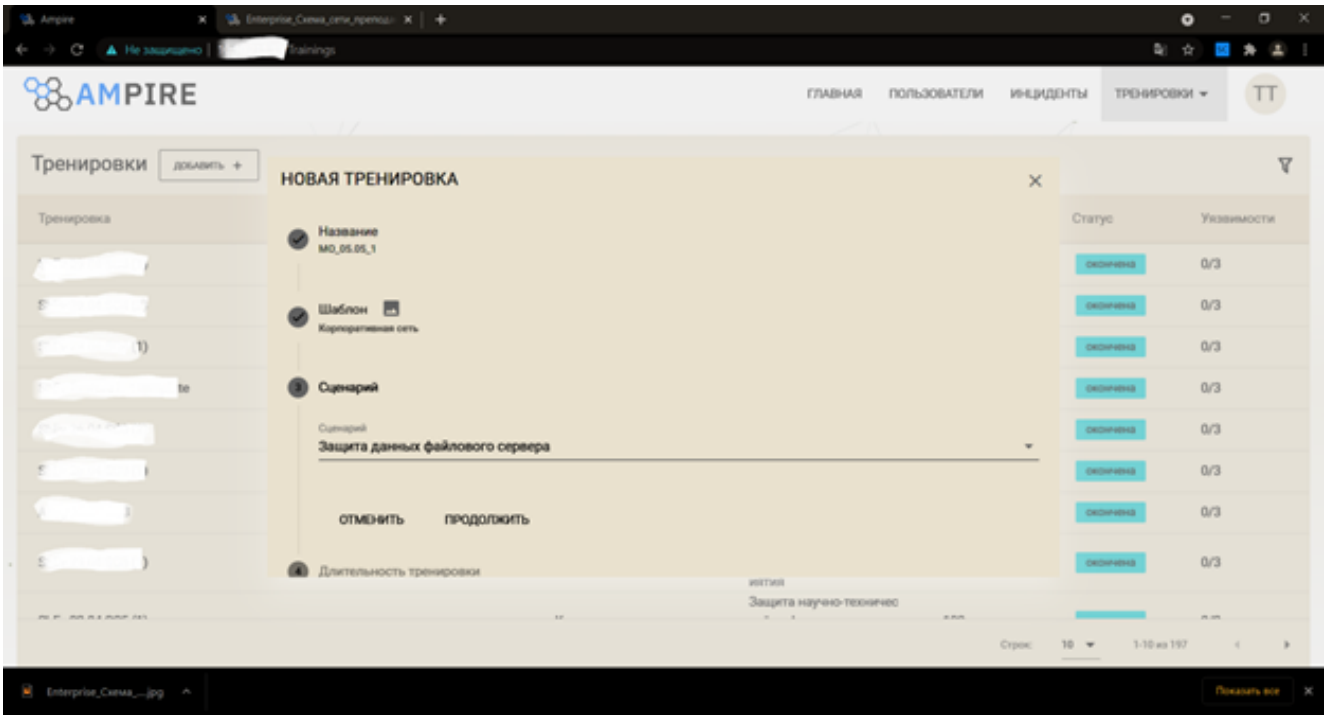

Рисунок 2-10. Интерфейс ПАК «Ampire» в режиме задания сценария КА новой тренировки)

В ПАК «*Ampire*» реализованы следующие функции:

- создание экземпляров КС на базе имеющихся шаблонов;
- управление пользователями, которые проходят обучение (создание профиля, распределение по группам, редактирование и удаление);
- управление виртуальными нарушителями (активация действий, остановка, выполнение отдельных шагов);
- создание тренировок, в которых объединяются экземпляры КС, пользователи и виртуальные нарушители;

- получение информации о ходе запущенных тренировок (количество и содержимое заведенных карточек инцидентов, статус по устранению имеющихся уязвимостей в экземплярах ИС, работоспособности инфраструктуры ПАК «*Ampire*»);

  взаимодействие между пользователями посредством встроенного мессенджера и системы тикетов;
- оценка качества работы обучаемых;
- вывод статистической информации из ПАК «*Ampire*» по результатам проведенных тренировок.

ПАК «*Ampire*» (*Academic*) включает в свой состав серверное оборудование, демонстрационное оборудование и ПО. Шаблоном ИС в ПК «*Ampire*» является набор виртуальных машин (серверы, рабочие станции, сетевое оборудование и т.д.), которые моделируют работу типовой КС организации (например, предприятие топливно-энергетической сферы, офис, КФС). Состав ПАК «*Ampire*» (*Academic*) приведен в таблице 2-5.

Таблица 2-5. Состав ПАК «*Ampire*» (*Academic*)

№	Технические характеристики	Кол-во, шт.
1	**ПАК «*Ampire*» (*Academic*) в составе:**	**1**
1.1	**Серверное оборудование**	
1.1.1	Сервер *Dell PowerEdge R540* в составе: – Процессор: *Intel Xeon Silver 4210 (2.20 GHz, 10 cores, 14 MB L3, 2400 MHz, 85W)* – 2 шт. – Оперативная память: 32Gb *PC4-21300(2666MHz) DDR4 ECC RDIMM* – 8 шт. – *SSD* Жесткие диски: *800GB SSD SATA Mix Use MLC 6Gbps HS 2.5" in 3.5" Carrier* – 6 шт. – *120GB SSD SATA Boot 6Gbps HS 2.5" in 3.5" Carrier* – 2 шт. – *RAID*-контроллер: *PERC H740p RAID (0,1,5,6,10,50,60) Controller 8Gb NV Cache 12Gb/s with battery* – 1 шт. – Модуль управления: *iDRAC 9 Enterprise* – 1 шт. – Сетевая карта: *Broadcom 5719 4x1Gb* – 1 шт. – Модуль питания: *Power Supply, 750W, Hot-plug* – 2 шт.	1
1.1.2	Коммутатор доступа *MES2428P*	1
1.1.3	Шкаф серверный 18*U* с глубиной 1000 мм напольного исполнения	1
1.1.4	Набор патчкордов для коммутации (30 шт.)	1
1.2	**Демонстрационное оборудование**	
1.2.1	Стойка для телевизора	1
1.2.2	Телевизор *LG 75SK8100 75"* (189 см)	1

1.2.3	Ноутбук *MSI GL63* в составе: – Процессор: *Intel Core i7-8750H 2.2 GHz* – Оперативная память: 8192 Мб, *DDR4* – *SSD* Жесткий диск: 128 ГБ – Жесткий диск: 1000 ГБ – Видеокарта: *nVidia GeForce GTX 1050, 2048 Мб, GDDR5*	1
1.3	**Лицензии на прикладное и системное ПО**	
1.3.1	*VMware 6 Essentials Kit for 3 hosts (Max 2 processors per host) VS6-ESSL-KIT-C*	1
1.3.2	*Basic Support/Subscription 6 Essentials Plus Kit for 1 year VS6-ESP-KIT-G-SSS-C*	1
1.3.3	ОС *Microsoft Windows* 10	10
1.3.4	ОС *Microsoft Windows Server Standard* 2019	5
1.3.5	*Microsoft Exchange Server 2019*	1
1.4	**Программное обеспечение ПАК «*Ampire*»**	
1.4.1	Система управления платформой «*Ampire*» на базе веб-приложения, включающая роли администратора, преподавателя и обучаемого	1
1.4.2	Типовой шаблон «Предприятие топливно-энергетической сферы» информационной системы, моделирующий работу предприятия, включающий офисный и промышленный сегменты.	1
1.4.3	Набор из 6-ти сценариев действий внешнего и внутреннего нарушителя и их автоматическая реализация	1
1.4.4	Количество виртуальных машин в шаблоне	23
1.4.4	Генератор сценариев (КА) для возможности вариативности действий нарушителя	1
1.5	**Академическая лицензия на ПО ПАК «*Ampire*»**	1
1.5.1	Количество одновременно подключаемых пользователей с ролью «преподаватель»	1
1.5.2	Количество одновременно подключаемых пользователей с ролью ««студент»	25

Подробное описание возможностей ПАК «*Ampire*» приведено в приложении G.

2.5.2. Методика проведения натурного моделирования компьютерной атаки

При проведении натурного моделирования динамики развития КА был реализован следующий сценарий целевой КА на инфраструктуру организации, схема которой представлена на рисунке 2-11.

Внешний нарушитель находит в сети Интернет-сайт организации и принимает решение о проведении КА на него с целью получения доступа к внутренним ресурсам. Обнаружив и проэксплуатировав уязвимость на Интернет-сайте, нарушитель получает доступ к серверу, который помимо основной информационной задачи предоставляет пользователям организации инструмент для генерации отчетов. С помощью этого вектора нарушитель пытается получить доступ на рабочие машины сотрудников. Главная цель КА – сделать дамп

корпоративной БД. Проводимая КА считалась идеальной, поэтому действия специалистов ИБ по обнаружению и блокировке нарушителя, и устранению последствий КА не предполагались. Событие ИБ характеризовалось:

- временем реализации действия нарушителем;
- этапом КА в соответствие с *Cyber Kill Chain* [126, 127] является временной интервал, в течение которого было реализовано действие нарушителя;
- описанием действия нарушителя;
- результатом, достигнутым нарушителем в результате реализованной КА.

Описанный сценарий КА был реализован в виде скрипта, имитирующего действия потенциального нарушителя. Минимальная задержка между реализацией различных методов КА и составляла 5 минут. Логирование всех действий нарушителя осуществлялось пользователем, имеющим статус «преподаватель».

Далее проводился анализ файла, содержащего информацию о событиях ИБ, с целью вычисления значений зависимости относительного числа «зараженных узлов» от времени. При этом было принято во внимание, что целью КА является не нарушение доступности, но нарушение конфиденциальности, т.е. получение дополнительной информации об «узле». В этой связи получение доступа к любому из 7 уровней модели *OSI* соответствующего автоматизированного рабочего места рассматривалось как событие доступа КА, состоящее в получении доступа нарушителя к узлу КС. Отметим, что обнаруженная уязвимость и ее эксплуатация, рассматривались как дополнительная информация, которая учитывалась при расчете количества «зараженных узлов».

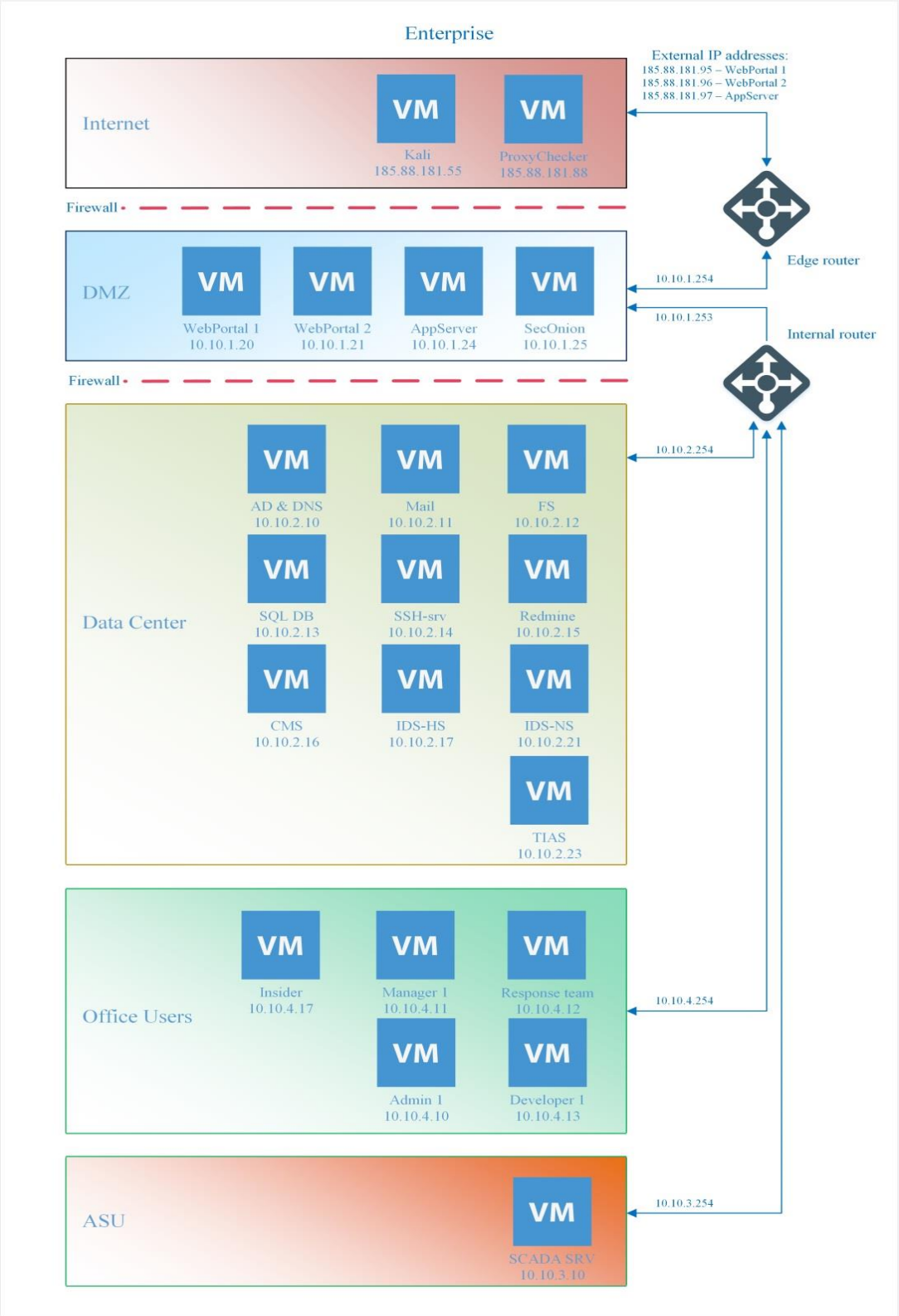

Рисунок 2-11. Схема стенда организации, на которой реализуется сценарий КА

2.5.3. Анализ результатов моделирования динамики развития компьютерной атаки

Журнал событий ИБ, сформированный в ходе проведения натурного моделирования КА, представлен в таблице 2-6. Здесь зараженным узлом считается узел, на котором злоумышленник получил доступ к одному из уровней модели *OSI* виртуальных машин стенда. В том случае, когда зараженный узел зараженный узел КС далее дополнительно применяет новый метод реализации КА на следующий узел КС, число зараженных узлов увеличивается на 0.5 (так как при выборе нового метода проведения КА с вероятностью 0.5 данная КА будет либо успешной, либо нет).

Таблица 2-6. Журнал зарегистрированных событий ИБ в ходе натурного моделирования КА

№ события	Время реализации КА	Этап КА	Описание этапа КА	Действие нарушителя	Количество «зараженных узлов», нарастающим итогом
1	7:37:55	0	Подготовка к проведению КА	Подготовка к проведению КА	0
2	7:38:25	0	Подготовка к проведению КА	Подготовка к проведению КА	0
3	7:38:55	1	Сканирование внешней сети организации, поиск открытого порта 80	Начало КА на сеть 185.88.181.0/24	0,5
4	7:40:01	1	Сканирование внешней сети организации, поиск открытого порта 81	Обнаружен веб-сервер (185.88.181.88, 185.88.181.95, 185.88.181.96, 185.88.181.97)	4,5
5	7:40:31	1	Сканирование внешней сети организации, поиск открытого порта 82	Не удалось подключиться к 185.88.181.88	4,5
6	7:42:12	1	Сканирование внешней сети организации, поиск открытого порта 83	Не удалось подключиться к 185.88.181.97	4,5
7	7:42:22	2	Эксплуатация уязвимости на веб-ресурсе и получение доступа к *DMZ*	Попытка эксплуатации уязвимости на 185.88.181.96	5
8	7:42:33	2	Эксплуатация уязвимости на веб-ресурсе и получение доступа к *DMZ*	*WebShell* загружен, эксплуатация уязвимости прошла успешно	6
9	7:44:23	2	Подготовка полезной нагрузки, загрузка ее на веб-сервер	Подготовка полезной нагрузки	6,5
10	7:46:53	2	Подготовка полезной нагрузки, загрузка ее на веб-сервер	Жду запуска файла администратором	6,5
11	7:49:08	3	Сканирование сегмента внутренней сети в поисках сервисов	Начало сканирования внутренней сети	7

12	7:49:18	3	Сканирование сегмента внутренней сети в поисках сервисов	Сканирую подсеть 10.10.2.0/27	8
13	7:49:38	3	Сканирование сегмента внутренней сети в поисках сервисов	Обнаружен *ssh* по адресу 10.10.2.15	9
14	7:49:58	3	Сканирование сегмента внутренней сети в поисках сервисов	Обнаружен *ssh* по адресу 10.10.2.23	10
15	7:50:18	3	Сканирование сегмента внутренней сети в поисках сервисов	Обнаружен *ssh* по адресу 10.10.2.13	11
16	7:50:28	3	Сканирование сегмента внутренней сети в поисках сервисов	Обнаружен *ssh* по адресу 10.10.2.14	12
17	7:50:38	3	Сканирование сегмента внутренней сети в поисках сервисов	Сканирование подсети 10.10.2.0/27 завершено	12
18	7:51:38	4	Подбор пароля для подключения к *ssh*-серверу у базы данных и получение доступа к файловой системе	Начало перебора паролей к *ssh*-серверу	12,5
19	7:51:43	4	Подбор пароля для подключения к *ssh*-серверу у базы данных и получение доступа к файловой системе	Перебор паролей на 10.10.2.23	12,5
20	7:51:44	4	Подбор пароля для подключения к *ssh*-серверу у базы данных и получение доступа к файловой системе	Пароль к *ssh* не найден на 10.10.2.23, пробую следующий сервер *Medusa v*2.2	12,5
21	7:51:45	4	Подбор пароля для подключения к *ssh*-серверу у базы данных и получение доступа к файловой системе	Перебор паролей на 10.10.2.13	12,5
22	7:53:49	4	Подбор пароля для подключения к *ssh*-серверу у базы данных и получение доступа к файловой системе	Пароль к *ssh*-серверу 10.10.2.13 успешно подобран *qwe123!@#*	13,5
23	7:53:54	4	Подбор пароля для подключения к *ssh*-серверу у базы данных и получение доступа к файловой системе	Перебор паролей на 10.10.2.14	13,5
24	7:54:45	4	Подбор пароля для подключения к *ssh*-серверу у базы данных и получение доступа к файловой системе	Пароль к 10.10.2.14 успешно подобран *q123!@#*	14,5
25	7:54:45	4	Выполнение команды *history*, обнаружение пароля от базы данных	Выполнение команды *history*	16
26	7:54:46	4	Выполнение команды *history*, обнаружение пароля от базы данных	Выполнение команды history на *ssh*-серверах	17,5
27	7:54:54	4	Выполнение команды *history*, обнаружение пароля от базы данных	В выводе команды *history* на 10.10.2.14 отсутствуют данные для подключения	18,5
28	7:55:21	4	Выполнение команды *history*, обнаружение пароля от базы данных	Пароль к *mysql* найден *qwe123asd*	19,5
29	7:55:23	4	Выполнение команды history, обнаружение пароля от базы данных	Бот успешно похитил секреты вашей организации	19,5

30	7:58:24	4	Цели КА достигнуты	Заражено максимально возможное число узлов	19,5

Для удобства дальнейшего анализа моменты времени, указанные в таблице таблице 2–5, пересчитывались в новые значения временной сетки, у которой за начало отсчета выбран момент времени 7:37:55, за единицу отсчета – секунды (см. таблица 2-7.)

Таблица 2-7. Соответствие между моментами времени, в которые произошли события в ходе проведения КА, в абсолютном времени и выбранной системе измерения времени

№ события	Абсолютное время	Модифицированная временная шкала	№ события	Абсолютное время	Модифицированная временная шкала
1	7:37:55	0	16	7:50:28	753
2	7:38:25	30	17	7:50:38	763
3	7:38:55	60	18	7:51:38	823
4	7:40:01	126	19	7:51:43	828
5	7:40:31	156	20	7:51:44	829
6	7:42:12	257	21	7:51:45	830
7	7:42:22	267	22	7:53:49	954
8	7:42:33	278	23	7:53:54	959
9	7:44:23	388	24	7:54:45	1010
10	7:46:53	538	25	7:54:46	1011
11	7:49:08	673	26	7:54:47	1012
12	7:49:18	683	27	7:54:54	1019
13	7:49:38	703	28	7:55:21	1046
14	7:49:58	723	29	7:55:23	1048
15	7:50:18	743	30	7:58:23	1228

Зависимость относительного числа зараженных узлов КС от времени (отношение числа зараженных узлов к общему числу узлов), характеризующая, как показано в разделе 2.4, динамику изменения КА, вычисленная на основе данных, представленных в таблице 2-6, 2-7, представлена на рисунке 2-12.

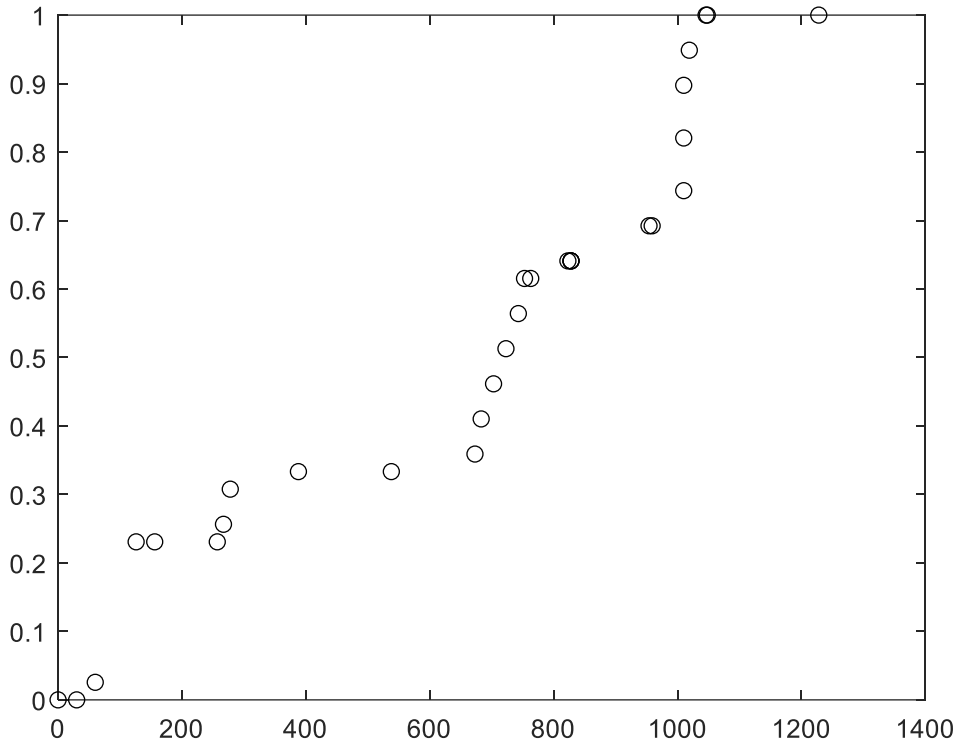

Рисунок 2-12. Зависимость относительного числа зараженных узлов КС от времени при натурном моделировании КА

Результаты аппроксимации эксперементальных данных, приведенных на 2-12, *s*-образными кривыми Перла-Рида (2.22) в соответствие с методом наименьших квадратов, обсуждаются представлены в разделе 2.4.2.4.

2.5.4. Результаты аппроксимации экспериментальной зависимости числа зараженных узлов от времени

Визуальный анализ зависимости числа зараженных узлов от времени, представленной на 2-12, позволяет предположить, что данная зависимость может быть аппроксимирована фунцией вида (2.22), которая представляет собой набор *s*-образных кривых Перла-Рида, заданных на последовательных интервалах:

1-ый интервал, начало в 7 часов 36 минут 55 секунд, окончание в 7 часов 40 минут 22 секунда;

2-й интервал, начало в 7 часов 40 минуты 31 секунда, окончание в 7 часов 46 минут 53 секунды;

3-й интервал, начало в 7 часов 46 минут 53 секунды, окончание в 7 часов 51 минуту 43 секунды;

4-й интервал, начало в 7 часов 51 минуту 43 секунд, окончание 7 часов 58 минут 23 секунды.

Далее на каждом из выбранных временных интервалов в соответствие с методом наименьших квадратов были вычислены параметры *s*-образных кривых Перла-Рида, аппросимировавшиеся на выбранных временных интервалах функциями

$$y_k(t) = \alpha_1^{\langle k \rangle} + \frac{\alpha_2^{\langle k \rangle}}{1 + \alpha_3 e^{-\alpha_4^k \left(t - t_0^{\langle k \rangle}\right)}}, \tag{2.26}$$

где

$k = \overline{1,4}$ – номер интервала аппроксимации.

Значения коэффициентов аппроксимирующих функций $\alpha_j^{\langle k \rangle}$, $j = \overline{1,4}$ находились из условия:

$$\underset{\alpha_1^{\langle k \rangle}, \alpha_2^{\langle k \rangle}, \alpha_3^{\langle k \rangle}, \alpha_4^{\langle k \rangle}}{\arg} \min \left(\sum_{i=1}^{N^{\langle k \rangle}} \left(y_i - \left(\alpha_1^{\langle k \rangle} + \frac{\alpha_2^{\langle k \rangle}}{1 + \alpha_3^{\langle k \rangle} \exp\left(-\left(\alpha_4^{\langle k \rangle} \left(t_i - t_1 \right) \right) \right)} \right) \right) \right)^2, \tag{2.27}$$

где

$N^{\langle k \rangle}$ – число отсчетов аппроксимируемой зависимости, укладывающихся на *k*-ом интервале, с помощью функции пакета MATДAD fminsearch.m.

Значения коэффициентов аппроксимирующих функций $\alpha_1^{\langle k \rangle}, \alpha_2^{\langle k \rangle}, \alpha_3^{\langle k \rangle}, \alpha_4^{\langle k \rangle}$, удовлетворяющих (2.27), представлены в таблице 2-8. Так как значения коэффициентов аппроксимирующих функций $\alpha_1^{\langle k \rangle}, \alpha_2^{\langle k \rangle}, \alpha_3^{\langle k \rangle}, \alpha_4^{\langle k \rangle}$, вычисленные с помощью одной из модификаций метода градиентного спуска, реализованного в функции пакета MATCAD fminsearch.m, также в таблице 2-8 приведены

использованные начальные приближения значений коэффициентов $\alpha_1^{\langle k\rangle}, \alpha_2^{\langle k\rangle}, \alpha_3^{\langle k\rangle}, \alpha_4^{\langle k\rangle}$.

Таблица 2-8. Значения коэффициентов аппроксимирующих функций $\alpha_1^{\langle k\rangle}, \alpha_2^{\langle k\rangle}, \alpha_3^{\langle k\rangle}, \alpha_4^{\langle k\rangle}$ аппроксимирующих функций

k	Начальное приближение				Значения коэффиентов			
	$\alpha_1^{\langle k\rangle}$	$\alpha_2^{\langle k\rangle}$	$\alpha_3^{\langle k\rangle}$	$\alpha_4^{\langle k\rangle}$	$\alpha_1^{\langle k\rangle}$	$\alpha_2^{\langle k\rangle}$	$\alpha_3^{\langle k\rangle}$	$\alpha_4^{\langle k\rangle}$
1	0	0,1	1,0	200,0	–0.0076	0.2409	0.0658	216.6173
2	0,2308	0,1	1,0	400,0	0.2241	0.10925	0.1862	15.3182
3	0,3333	0,1	5,0	10,0	0.3237	0.33365	0.0353	466.8322
4	0,6410	0,1	1,0	40,0	0.6503	0,3720	0,0560	23712.73138

Результаты аппроксимации зависимости относительного числа зараженных узлов от времени представлены на рисунке 2-13.

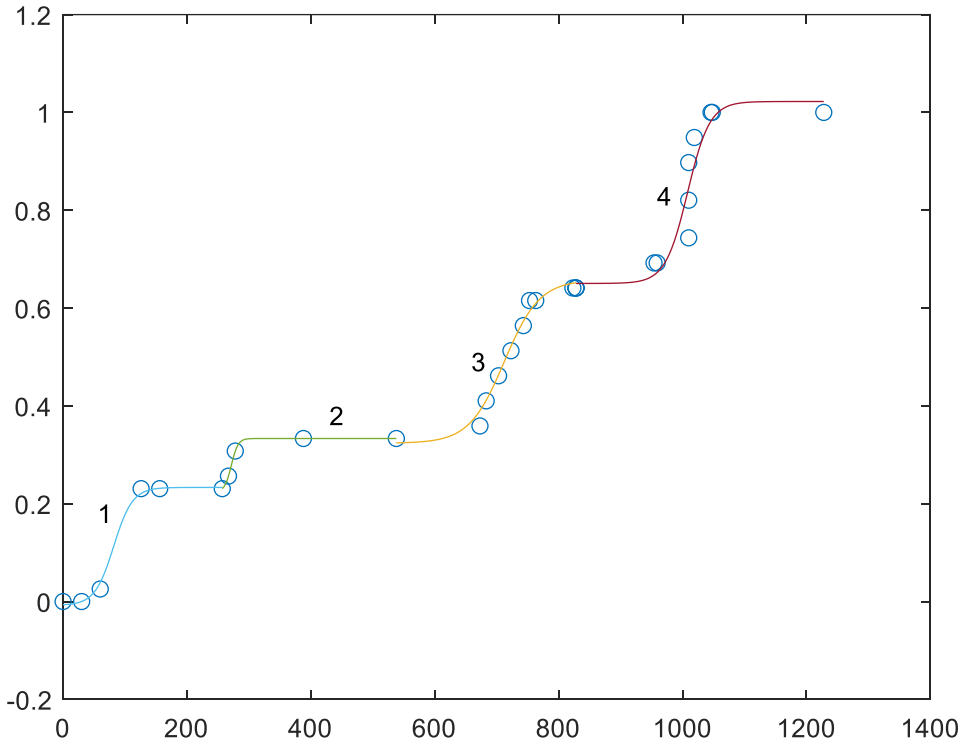

Рисунок 2-13. Результаты аппроксимации зависимости количества зараженных узлов на каждом этапе натурного моделирования каскадной моделью s-образных кривых Перла-Рида

Из рисунка 2–13 видно, что, действительно, динамика заражения узлов КС, которая в развиваемой нами модели эквивалентна динамики изменения вероятности реализации КА от времени на этапе прогнозирования, может быть описана с помощью каскадной математической модели (2.22).

Для их практического использования данного результата необходимо разработать рекомендации для оценивания параметров в (2.21), (2.22).

2.6. Разработка рекомендаций для оценивания параметров математических моделей, описывающих динамику компьютерной атаки

2.6.1. Этапы реализации компьютерной атаки

Для обоснования рекомендаций по оцениванию параметров математических моделей, описывающих динамику КА, проведем анализ существующих подходов к определению этапов и методов КА существующих моделей угроз ИБ и КА: *Cyber Kill Chain* [126, 127], *NIST 800-115* [128], *Mitre Att&ck* [129], *Certified Ethical Hacker (CEH)* [130], методология ФСТЭК России [5-7] и методологии *ISO 27001* [13], а также проведем их адаптацию к нашей модели рассмотрения КА с точки зрения нарушителя.

В методологиях *Cyber Kill Chain* [126, 127], *NIST 800-115* [128], *CEH* [130] под угрозой понимается последовательность этапов действий, начиная с разведки и заканчивая действиями нарушителя по достижению поставленной им цели. Под целью нарушителя подразумевается нарушение конфиденциальности, целостности и/или доступности информации или компонентов ИС организации. Для каждого этапа нарушитель использует различные методы. Отметим, что методологии *NIST 800-115* [128] и *CEH* [130] определяют этапы проведения тестирования на проникновение, т.е. эмулирование.

Выделенные этапы проведения КА в соответствии методологиями *Cyber Kill Chain* [126, 127], *NIST 800-115* [128], *CEH* [130] представлены в таблице 2-9.

Таблица 2-9. Этапы КА, выделенные в соответствие с методологиями *Cyber Kill Chain [126, 127], NIST 800-115 [128], CEH [130]*

Обобщенные	*Cyber Kill Chain* [126,	*NIST 800-115* [128]	*CEH* [130]

этапы КА	127]		
Теоретическая подготовка – объединяет в себя этапы, связанные с изучением объекта КА и подготовкой к КА	Этап «*Reconnaissance*» – Разведка. Включает в себя исследование, идентификацию и выбор объекта КА. Этап «*Weaponization*» – Вооружение. Включает выбор и подготовку инструментов и ВПО для совершения КА.	Этап «*Planning phase*» – Планирования. Определяются правила, а также устанавливаются цели тестирования. Этап «*Discovery phase*», включающий в себя 2 части. Первая часть – начало реального тестирования и охватывает сбор и сканирование информации. Вторая часть – анализ уязвимостей, который включает в себя сравнение служб, ПО и ОС просканированных узлов с базами данных уязвимостей.	Этап «*Reconnaissance*» – Пассивная и активная разведка. Предполагает сбор информации о потенциальном объекте КА без обнаружения, включая сбор информации с общедоступных источников, отслеживание сетевого трафика и зонирование сети организации. Этап «*Scanning*» – Сканирование. Подтверждение информации, обнаруженной во время разведки, и ее использование для исследования сети.
Практическая подготовка – объединяет этапы, связанные с практической реализации подготовительной части КА	Этап «*Delivery*» – Доставка. Донесение вредоносного контента до целевой системы. Этап «*Exploitation*» – Эксплуатация уязвимости системы. Этап «*Installation*» – Инсталляция. Открытие удаленного доступа и другие действия с зараженной системой Этап «*Command and Control*)» – Получение управления. Управление зараженной системой.	Этап «*Gaining access*» – Получение доступа. Этап «*Escalating Privileges*» – Повышение полномочий доступа. Этап «*System Browsing*» – Получение доступа/управление целевой системой. Этап «*Install Addition Tools*» – Установка/запуск дополнительного ПО. На этих этапах проводится проверка идентифицированных на этапе «*Discovery phase*» уязвимостей путем их эксплуатации.	Этап «*Gaining access*» – Получение доступа. Уязвимости, обнаруженные на этапе разведки и сканирования, теперь используются для получения доступа к целевой системе.
Достижение цели КА – связано с практической реализацией цели КА, в том числе, причинение вреда	Этап «*Actions on Objective*» – Выполнение действий. Сбор, кража, отправка данных, шифрование файлов, подмена и удаление данных.	Этап «*Reporting*» – Подготовка отчета. Фиксация уязвимостей, эксплуатация которых может привести к успешной реализации реальной КА.	Этап «*Maintainig access*» – Реализация цели КА. Получение управления, сохранение доступа для будущих КА и реализация текущих целей КА.

Из таблицы 2-9 видно, что у обсуждаемых методологий имеется общий этап, несвязанный с воздействием нарушителя на объект КА – этап теоретической подготовки. В рамках этого этапа нарушителем занимается сбором общедоступной информации, а также изучением инструментов и методов реализации КА. Данная работа схожа с работой исследователя, поэтому, даже, выявив подобную активность, достаточно трудно привлечь нарушителя к ответственности.

Второй этап – практическая подготовка, который хоть и связан с активными действиями нарушителя, направленными на объект КА, однако, не приносит «видимого» вреда, а значит, не приводит к обнаружению – обращению в правоохранительные органы [131, 132].

Третий этап связан с непосредственным нарушением свойств критической (защищаемой) информации. Особенность двух последних этапов заключается в том, что выявленная на первом этапе уязвимость и подготовленный эксплойт по ее эксплуатации на этапе практической реализации КА не гарантирует получение нарушителем запланированного результата. Соответственно, в ходе реализации КА присутствует «петля» или откат к предыдущему этапу для дополнительной подготовки.

Отметим, что методики КА, связанные с сокрытием следов присутствия нарушителя, мы не выделяем в отдельный этап КА, так как нарушитель стремится их использовать на каждом этапе проведения КА. Кроме того, нарушитель может защищать целевую систему от других нарушителей или специалистов ИБ, поддерживая эксклюзивный доступ с помощью специального ВПО, например, с целью получения выкупа.

В соответствии с технологией *Cyber Kill Chain* [126, 127] известно, что прервать КА можно на любом из этапов, разорвав цепочку действий нарушителя, ведущих его к цели КА. Данные методологии рассматривают КА, в первую очередь, с точки зрения подбора механизмов и средств защиты, но его можно рассмотреть и с точки зрения нарушителя. КА может быть технически прекращена нарушителем:

– если у него будет недостаточно навыков, методов и инструментов для проведения КА, либо они не будут успешно реализовываться на любом из этапов КА.
– если КА будет обнаружена на этапе теоретической или практической подготовки.

Проверим применимость ТДИ [48] к делению КА на этапы с точки зрения нарушителя в соответствии методологиями *Cyber Kill Chain* [126, 127], *NIST 800-115* [128], *CEH* [130]. Для этого обратимся к пяти этапам принятия решения о возможности использования метода КА, при этом указав места их реализации:

1. Теоретическая подготовка – реализуется в сетях *DarkNet* (в терминах ТДИ включает этапы: Знание, Убеждение, Принятие решения). В соответствии с ТДИ выявить возможность применения метода КА нарушителем на этом этапе можно только анализируя данные в *DarkNet*.

2. Практическая подготовка – реализуется в сетях организации (в терминах ТДИ включает этап: Применение). В соответствии с ТДИ выявить возможность применения метода КА нарушителем на этом этапе можно путем анализа журналов регистрации событий ИС и средств ЗИ организации. Причем, тестирование метода нарушитель может проводить не обязательно на целевой организации.

Таким образом, по данным центров мониторинга инцидентов ИБ, систем по сбору статистики со средств защиты можно проследить динамику развития возможности применения конкретного метода КА во времени, используя функцию динамики распространения инновации.

3. Достижение цели КА – реализуется в сетях организации (в терминах ТДИ включает этап: Подтверждение). В соответствии с ТДИ метод КА, достигнувший этого этапа, удовлетворяет основным свойствам инновации.

В соответствии с ТДИ нарушителей можно разделить по признаку индивидуальной предрасположенности к восприятию нового метода КА. Таким образом, выявив методы КА, реализуемые нарушителями новаторами и ранними

последователями, мы можем предупредить применение метода КА на большую часть организации.

Выявляя КА на первом и втором этапе ее реализации, возможно предупредить нанесение ущерба организации, а также увеличить вероятность и величину наказания для нарушителя, что повлечет за собой снижение ожидаемой полезности от КА, тем самым сократит их вероятность.

С нашей точки зрения, прогнозирование вектора КА корректнее реализовывать на этапе теоретической подготовки нарушителя к проведению КА, так как такой подход позволит выявить его на этапе практической подготовки к проведению КА, предотвратить и передать информацию в правоохранительные органы. В этой связи прогнозирование вектора КА будем реализовывать на этапе теоретической подготовки нарушителя к проведению КА.

2.6.2. Методы компьютерной атаки

Существующий подход к определению методов КА

База *Mitre Att&ck (Adversarial Tactics, Techniques & Common Knowledge)* была создана в 2013 г. для «составления структурированной матрицы используемых киберпреступниками приемов, чтобы упростить задачу реагирования на киберинциденты» [129]. Она содержит структурированный список тактик, техник и общеизвестных фактов о нарушителях, разделенный на группы в зависимости от этапа и цели использования, представленный в виде матрицы. Классификация методов, в соответствии с методологией *Mitre Att&ck,* проведена на основе задачи, реализуемой нарушителем на объект КА, список которых содержит:

- получение первоначального доступа (*Initial Access*);
- выполнение (*Execution*);
- закрепление (*Persistence*);
- повышение привилегий (*Privilege Escalation*);
- обход защиты (*Defense Evasion*);
- получение учетных данных (*Credential Access*);

– обнаружение (*Discovery*);
– боковое перемещение (*Lateral Movement*);
– сбор данных (*Collection*);
– эксфильтрация или утечка данных (*Exfiltration*);
– управление и контроль (*Command and Control*);
– влияние (*Impact*).

Рисунок 2-14. Структурная схема канала реализации угрозы

Напомним, что в методологии ФСТЭК России [5] под понятием «угроза безопасности информации» подразумевается «совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа» к информации. Результатом такого доступа могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение информации, а также иные неправомерные действия при их обработке информации в информационной системе. При этом, априори, полагается, что каждая из угроз формируется взаимосвязью источников угроз, способов реализации угроз, уязвимостей и последствий [5-7]. Обобщённая схема канала реализации угроз БИ представлена на схеме Рисунок 2-14.

При формировании перечня угроз БИ необходимо использовать банк данных угроз ФСТЭК России (более 200 угроз) [6], который в терминах *Mitre Att&ck* [129] представляет собой перечень возможных уязвимостей объектов КА (содержит информацию о более чем 27 тыс. уязвимостей) и методов реализации КА.

Отметим, что помимо формирования перечня угроз БИ особое внимание необходимо также уделять оценке опасности реализации данной угрозы ИБ. Опасность реализации угрозы определяется, например, степенью негативных последствий для субъектов ПД. Действительно, любая система ЗИ, в том числе, предназначенная для обнаружения нарушителей, в первую очередь, нацелена на выявление действий, направленных против защищаемой информации, в частности

ПД. При этом в соответствие с методологией *ISO 27001* [13] риски ИБ, меньшие некоторого приемлемого уровня, считаются приемлемыми. Такой уровень может быть у активов с низкой ценностью для организации. В результате КА на информационные ресурсы, не относящиеся к ценным активам для данной организации, может пройти незамеченной. Анализ фиксации обращений в правоохранительные органы по факту киберпреступлений показывает, что они происходят только в случае нарушения свойств критичной (защищаемой) организацией информации. Таким образом, существующий подход по определению методов КА не обеспечивает полноту и актуальность реально используемых методов КА.

Определение методов компьютерной атаки, на основе анализа данных из DarkNet

При моделировании КА с точки зрения нарушителя следует учитывать информацию, которой обладает и может использовать нарушитель. В разделе 2.3 приведено обоснование с точки зрения ТДИ возможности использования данных из *DarkNet* для прогнозирования возможности КА.

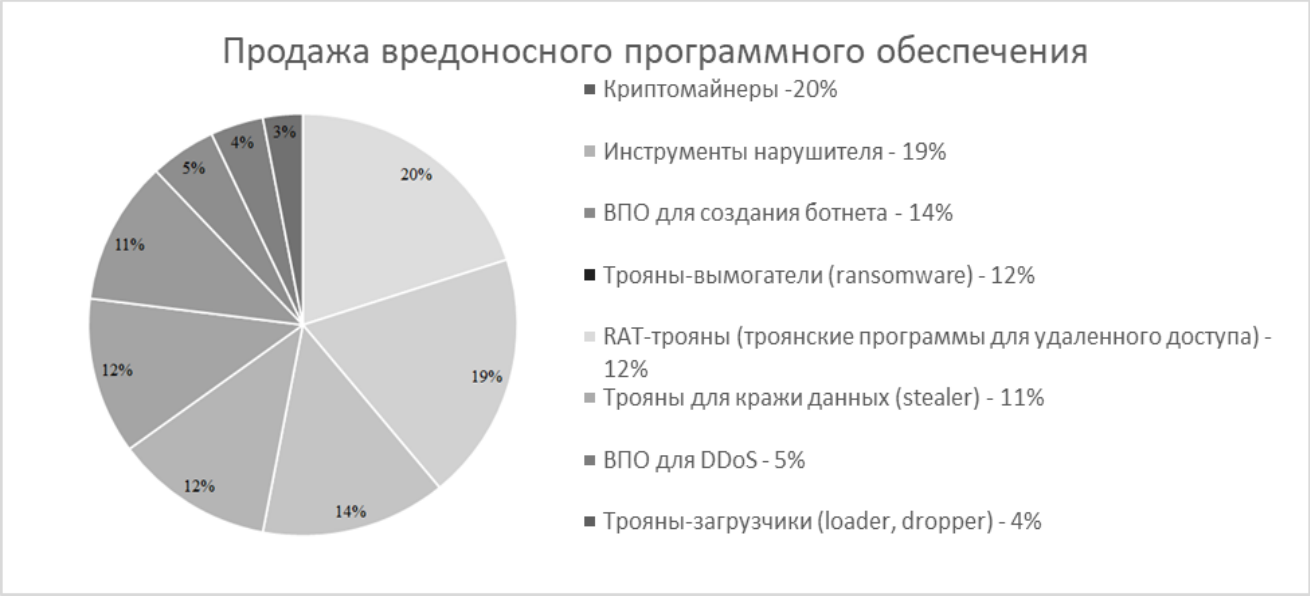

Рисунок 2-15. Процентное соотношение продаваемых методов и инструментов для реализации КА в *DarkNet*

Анализ результатов исследований *DarkNet* [35, 133-135] показывает, что на форумах *DarkNet*, в первую очередь, обсуждаются эксплоиты[1] и утилиты[2], которые используются для КА. Среди наиболее обсуждаемых утилит оказывается ПО для создания вирусов, которые могут обходить системы ИБ, ПО для подбора паролей и удаленного администрирования. Наибольшее число эксплоитов, упоминаемых на форумах *DarkNet* относится к ИБ сетевой инфраструктуры и ОС, около 15% – к веб-приложениям и мобильным технологиям [35].

На форумах и чатах *DarkNet* активно обсуждается продажа следующих категорий [35, 133–135]:

- продажа ВПО;
- продажа эксплойтов;
- продажа данных;
- продажа доступов, т.е. сведений, с помощью которых можно осуществить несанкционированный доступ к сайту или серверу с последующей возможностью загрузки файлов или выполнения команд;
- продажа услуг.

Стоимость различного ПО и услуг в *DarkNet* варьируется от 1$ до 2540$. На рисунке 2-15 представлено процентное соотношение упоминаний о различных методах и инструментах реализации КА.

На рисунке 2-16 представлено процентное соотношение данных о продаже различных услуг. Более подробная информация о методах КА, обсуждаемых в сети *DarkNet,* приведена в приложении F.

Анализ полученных данных позволяет сделать вывод, что выбор конкретного метода проведения КА определяется:

- наличием и известностью метода КА, в том числе в *DarkNet*;
- отсутствием мер защиты от КА;

---

[1]Эксплоит – компьютерная программа или фрагмент программного кода или последовательность команд, использующие уязвимости в ПО для проведения КА на ИС

[2]Утилита – вспомогательная компьютерная программа в составе общего ПО для выполнения специализированных типовых задач, связанных с работой оборудования и ОС

– не реализуются мероприятия по мониторингу КА;
– совместимостью с широко распространенной инфраструктурой организаций;
– отсутствием видимого вреда для объекта КА.

Анализ ВПО [135] показал, что данный тип ПО легко масштабируется, адаптируясь к различной инфраструктуре. Это дает возможность успешно применять старые вектора КА для новой архитектуры ИС (например, облачные технологии и *IoT*. По оценкам [135], количество совершенно нового вредоносного ПО, появившегося с июля 2016 по июнь 2018 гг., составило менее 10% от общего числа вредоносных программ. Причем распространение методов КА идет по формуле (2.21), что подтверждено на практических данных в разделе 2.4.

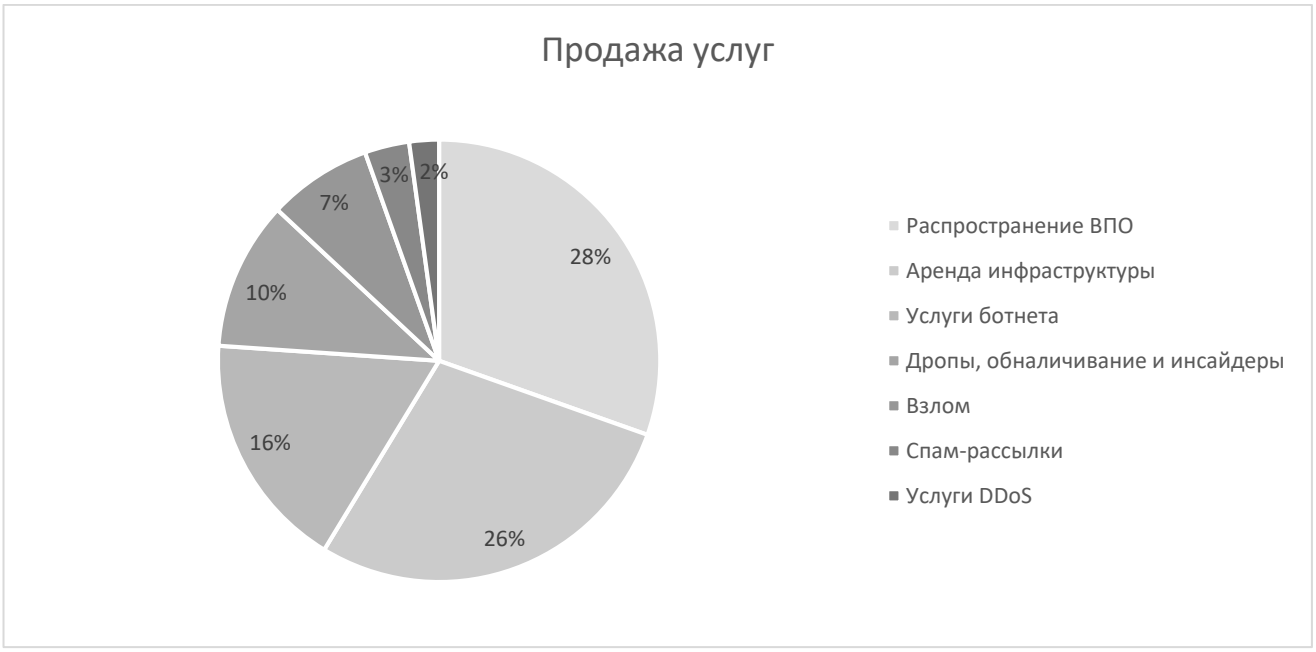

Рисунок 2-16. Процентное соотношение данных о продаже различных услуг для реализации КА в *DarkNet*

Следует отметить, что нам не удалось обнаружить работ, в которых описаны методы использования информации, извлеченной из *DarkNet*, для проектирования векторов КА.

2.6.3. Выбор характеристик компьютерной атаки, влияющих на возможность ее реализации

На основании вышеизложенных результатов выделим характеристики КА, определяющие на возможность ее реализации.

1. КА может быть начата нарушителем на этапе теоретической подготовки, если:

– нарушителю известен метод КА, в том числе из сети *DarkNet* (количественно данный фактор можно охарактеризовать коэффициентом известности метода КА a_n, зависящего от активности обсуждений («объяснений») данного метода КА на форумах *DarkNet*, который есть отношение числа всех обсуждений в указанном сегменте Интернет данного метода КА к общему числу обсуждаемых методов КА);

– нарушителю известна информация о практической апробации метода a_p, или успешной реализации аналогичной КА a_l;

– выгода от успешной реализации КА намного больше легального заработка.

В этой связи, прогнозирование вектора КА целесообразно проводить на этапе теоретической подготовки (см., также раздел 2.6.1).

Для подтверждения адекватности характеристик, определенных для этапа теоретической подготовки далее в разделе 2.6.5 будет проведен анализ КА, реализованной ВПО *Petya* на ИС, расположенные на территории Украины.

2.6.4. Выбор параметров функции изменения возможности реализации компьютерной атаки во времени

Определим, исходя из выше обоснованных характеристик, параметры функции изменения возможности реализации метода КА во времени из формулы (2.22). Эти параметры характеризуют динамику изменения возможности КА во времени, а также задержку в реализации метода КА от момента появления информации о возможности ее реализации. В соответствии с ТДИ скорость изменения диффузии по Э. Роджерсу [48] зависит от пяти основных свойств

инновации, которые потенциальные потребители оценивают при принятии решения, использовать инновацию или нет, приведенные в разделе 2.3.

Проведем аналогию данных свойств инновации со свойствами методов КА.

В соответствии с моделью Мэнсфилда [50] параметр α_j определяется:

- рентабельностью использования этого метода КА по сравнению с альтернативными методами (характеризуется W_m – выгода нарушителя в случае успешной реализации КА, W_j – текущий доход нарушителя от легальной деятельности, F_j – тяжесть наказания в случае разоблачения нарушителя (в денежном эквиваленте));
- инвестициями, необходимыми для реализации выбранного метода КА, измеряемые стоимостью C_j метода, оцениваемой на основе анализа информации в сетях *DarkNet* в процентах от средней общей суммы активов нарушителя.

В соответствии с моделью Басса [49] параметр β_j характеризуется на теоретическом этапе:

- рекламой в *DarkNet* с целью приобретения/использования рассматриваемого метода КА (определяется на первом этапе КА). В соответствии с моделью Басса [49] для новых методов КА это в первую очередь реклама – количество упоминаний в сетях *DarkNet* (известность метода КА в сети *DarkNet* a_n).
- данными межличностного взаимодействия нарушителей в *DarkNet*, которые уже приобрели/использовали рассматриваемый метод КА (определяется на втором этапе КА) a_l и практической апробацией метода КА a_p – совместимость с инфраструктурой атакуемой организации, сложностью реализации, появлением подтверждений применения/наказания при использовании данного метода КА в сети *DarkNet*, новостных агрегаторах, свой опыт тестирования.

2.6.5. Обоснование выбора источников первичной информации для расчета возможности реализации метода компьютерной атаки

Рассмотрим параметры, определяющие изменение во времени возможности реализации метода КА.

Параметр α_j – определяется рентабельностью использования метода КА по сравнению с альтернативными вариантами, в том числе, возможный легальный заработок. Возможный легальный заработок нарушителя W_j будем определять по средней заработной плате специалиста по тестированию на проникновения за рассматриваемый период. Заработок нарушителя от успешной реализации КА W_{mj} будем определять как среднее значение заработка нарушителя от КА подобного класса, данную информацию будем выявлять в новостных агрегаторах, за вычетом стоимости реализации КА, стоимость которой представлена в *DarkNet*.

Таким образом, чем выше рентабельность метода, тем больше вероятность его использования, т.е.

$$\alpha_j = \frac{\left(1-\rho_{nj}\right)\left(W_{mpj}+W_j\right)+\rho_{nj}\left(W_{mpj}+W_j-F_j\right)}{W_{mpj}-C_j} \qquad (2.28)$$

где

j – используемый метод КА;

C_j – стоимость КА в сетях *DarkNet*;

W_{mpj} – выручка нарушителя в случае успешной реализации КА;

W_i – текущий доход нарушителя от легальной деятельности;

W_{mj} – доход нарушителя от реализации j-ого метода КА, без учета затрат.

Параметр β_j – характеризует внешние (в виде рекламы в *DarkNet*) и внутреннее (межличностное взаимодействие, апробацию КА) воздействия на потенциальных нарушителей, определяющий инновационность и имитационную способность метода КА.

$$\beta_j = a_n + a_l + a_p, \qquad (2.29)$$

где

j – рассматриваемый метод КА;

a_n – известность метода КА в сети *DarkNet*;

a_l – коэффициент межличностной рекламы метода КА в *DarkNet* (успешности реализации аналогичных КА),

a_p – коэффициент апробации метода КА в *DarkNet* (успешная практическая проверка метода КА), оцениваемый на основе данных новостных агрегаторов и/или данных центров мониторинга ИБ.

Степень популярности данного метода КА в сети *DarkNet* a_n будем оценивать отношением числа его упоминаний A_{lp} к общему количеству рекламных сообщений за рассматриваемый период A_l:

$$a_l = \frac{A_{lp}}{A_l},$$

здесь

A_l – количество попыток реализации КА данного типа;

A_{lp} – количество успешно реализованных КА;

наличие практической апробации данного метода КА – отношение количества попыток его реализации A_p к общему числу попыток КА, зарегистрированных центрами мониторинга КА, A_{pp}, а также наличием и простоте реализации средств ЗИ (т.е. практическому применению средств ЗИ):

$$a_p = \frac{A_{pp}}{A_p}.$$

Научно обоснованная методика оценивания данных изложена далее в главе 3.

2.6.6. Оценка адекватности модели проведения компьютерной атаки на примере компьютерной атаки, реализованной с помощью вредоносного программного обеспечения *Petya*

Для подтверждения адекватности модели динамики КА рассмотрим сценарий проведения КА с помощью ВПО *Petya*. Впервые ВПО *Petya* было обнаружено в 2016 г. [117], а его широкомасштабное распространение началось в апреле 2017 г. [118]. Данное ПО использовало известную уязвимость *EternalBlue*, которая ранее уже эксплуатировалась для проведения КА шифровальщиком *WannaCry*. Это, с нашей точки зрения, является подтверждением наличия этапа «Практическая подготовка к проведению КА». Данный вывод также подтверждается результатами анализа форумов и чатов *DarkNet* в соответствующий период времени [35, 133-135], результаты которого свидетельствуют о том, что:

– осуществлялась продажа услуг, связанных, с подготовкой поддельных файлов якобы с обновлениями или утилитами, которые размещают на взломанных или подконтрольных нарушителю организациях в 51% случаев (из всех услуг, продаваемых в *DarkNet*);

– происходило обсуждение ВПО, связанного с Троянами-вымогатели (*ransomware*), к которым относится Petya (процент сообщений, связанных с этим типов ВПО, составлял 12% от общего числа сообщений), таким образом, для аналогичного КА ВПО *WannaCry* $\lim\limits_{t\to\infty}\rho_{nj}=0$, так как КА началась 12.05.2017, а практическое тестирование ВПО Petya, проведенное в апреле 2016 г. оказалось успешным.

Следовательно, в соответствии с формулой (2.29) до апреля 2016 г. $\beta_j=12$, $a_n=12, a_p=0, a_l=0$; с апреля 2016 г. до мая 2017 г. $\beta_j=12$, $a_n=12, a_p=100, a_l=0$; в мае 2017 г. $\beta_j=112$, $a_l=100$, в июне 2017 г. и далее $\beta_j=212$.

В период до апреля 2016 г., так как подтверждений возможности проведения незаметной КА не было, но Уголовный кодекс РФ [117], предусматривал штрафы и/или лишение свободы за совершение КА, $\rho_n=1$. При этом суммарная выручка нарушителя от КА, так как оценка применимости не была проведена, составлял $W_{mpj}=0$ руб. Текущий доход нарушителя от легальной

деятельности, оцениваемый как средняя зарплата специалиста в ИТ-отрасли, $W_j = 80000$. Соответственно, $F_j = 84 \cdot \left(W_j + W_{mj}\right)$ (см. приложение Е). $C_j = 16200$ (см. приложение F, Далее подставляя полученные оценки в (2.3), находим:

$$\alpha_j = \frac{\left(1-\rho_{nj}\right)\left(W_{mj}+W_j\right)+\rho_{nj}\left(W_{mj}+W_j-F_j\right)}{W_{mj}-C_j} =$$

$$\frac{\left(1-0\right)\cdot\left(80000\right)+0\cdot\left(0+80000-84\cdot 8000\right)}{0-16200} = -4{,}9.$$

График функции $Y(t) = \frac{1}{1-4.9e^{-12t}}$ представлен на рисунке 2-17.

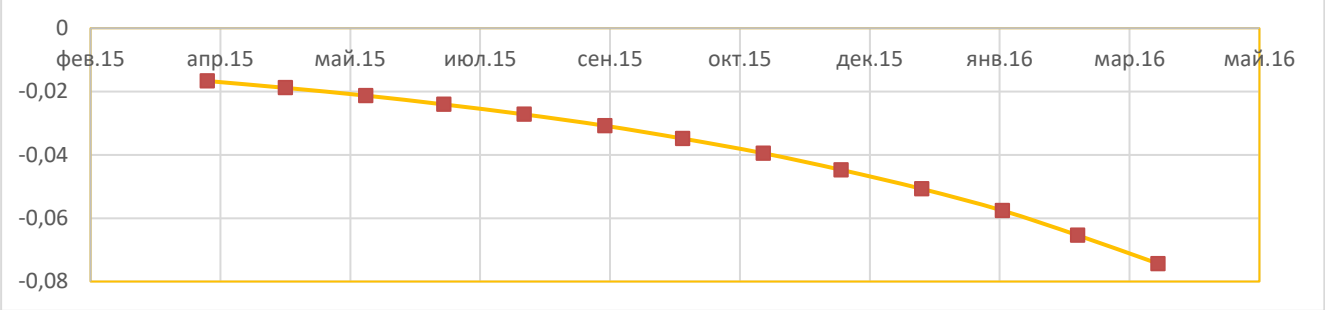

Рисунок 2-17. График функции $Y(t)$ в период с апреля 2015 г. по апрель 2016 г.

Из рисунка 2-17 видно, что несмотря на известность метода КА с помощью ВПО *Petya* и отсутствии его успешной апробации функция $Y(t)$ принимает только отрицательные значения и $\rho(A) \to 0$. Таким образом, в период теоретической подготовки затраты денежных средств на разработку методов по распространению КА ВПО *Petya*, делали проведение данного типа КА нерентабельной.

Далее нарушитель в период с апреля 2016 г. по май 2017 г. провел успешную апробацию КА ВПО *Petya*, наказания за которую не последовало. При этом, так как оценка возможности проведения данного типа КА ранее не была получена, суммарный заработок нарушителя от КАсоставил около $W_{mp} = 18000$ руб.

Для нарушителя, не склонного к риску вычисляем значение ожидаемой полезности на данном этапе в соответствие с последовательностью действий и

значениями параметров, обоснованными в разделе 2.2.5 (напомним, что при расчете заработка нарушителя от КА учитываем затраты на реализацию КА), по формуле, предложенной Бернулли [47]: $U(\xi) = b\ln\left(\frac{a+\xi}{a}\right)$. Так как в 2016 г. МРОТ составлял 6240 руб. [121], будем полагать, что $a = 6240, b = 1$:

$$EU_{\Sigma} = (1-\rho_n)U(W_m + W_j) + \rho_n U(W_m + W_j - F) =$$
$$= (1-0)\cdot\ln\left(\frac{18000-16200+80000+6240}{6240}\right) -$$
$$0\cdot\ln\left(83\cdot\left(\frac{18000-16200+80000+6240}{6240}\right)\right) = 2,64,$$

и далее значение параметра α_j:

$$\alpha_j = \frac{(1-\rho_{nj})(W_{mpj} + W_j) + \rho_{nj}(W_{mpj} + W_j - F_j)}{W_{mpj} - C_j} =$$
$$\frac{(1-0)\cdot(80000+18000) + 0\cdot(0+80000+18000-84\cdot(80000))}{18000-16200} = 54.$$

График функции $Y(t) = \frac{1}{1-54e^{-112t}}$ в период с апреля 2016 по май 2017 гг. представлен на рисунке 2-18.

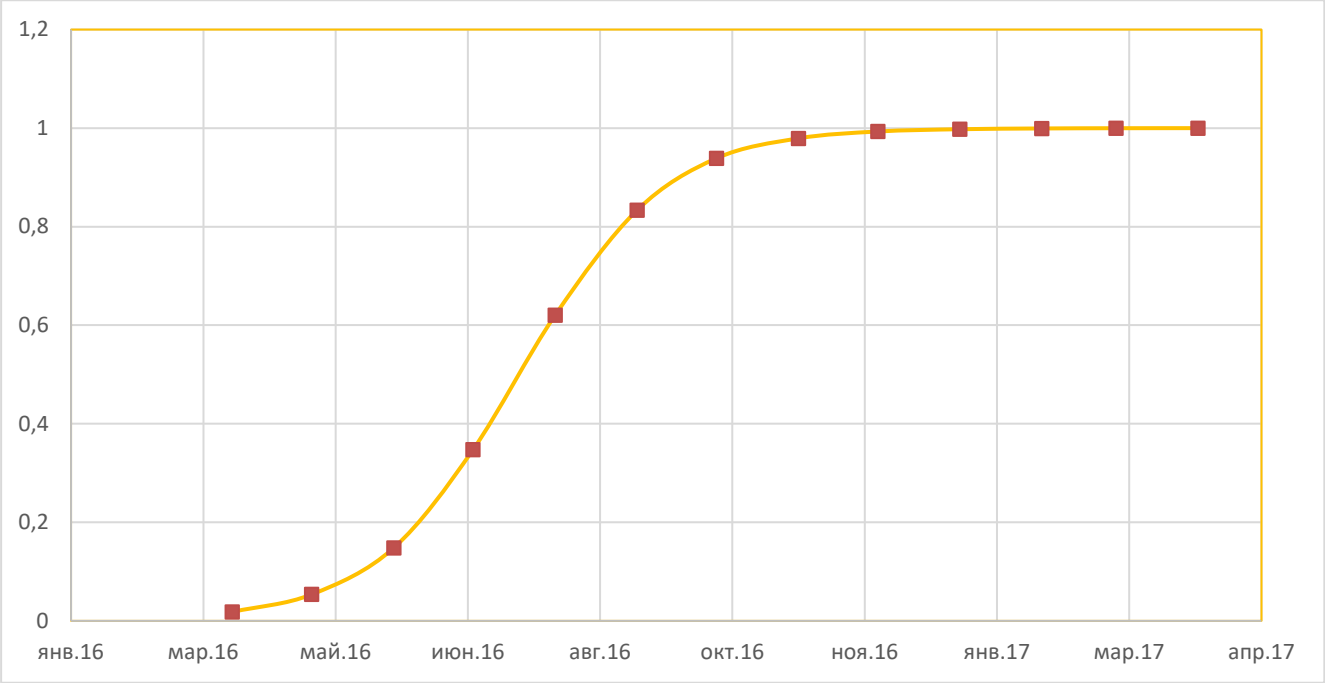

Рисунок 2-18. Динамика изменения вероятности использования КА ВПО *Petya* в период с апреля 2016 по май 2017

Из рисунка 2-18 видно, что начиная с ноября 2016 г. $p(A)\approx 1$. При этом ожидаемая полезность от нелегальной деятельности в период с апреля 2016 г. по май 2017 г. оказалось равной:

$$EU_{нл} = (1-\rho_n)U(W_m + W_j) + \rho_n U(W_m + W_j - F_j) =$$

$$(1-0)\cdot \ln\left(\frac{18000-16200+6240}{6240}\right) - 0\cdot \ln 83\cdot\left(\frac{18000-16200+6240}{6240}\right) = 0,25.$$

Следовательно, $\rho\left(\frac{EU}{A}\right) = \frac{EU_{нл}}{EU_{\Sigma}} = \frac{0,25}{2,64} \approx 0,09$.

Таким образом, при известности метода КА ВПО *Petya* и его успешной апробации нормированное значение $p(EU\,A) = \rho\left(\frac{EU}{A}\right)p(A) = 0,09 \quad \left(p(A)=1\right)$. Следовательно, выгода от реализации КА при атаке на единственную организацию оказалась меньше возможного легального заработка. В этой связи нарушитель осуществил успешный поиск методов единовременного запуска КА ВПО *Petya* на большом числе компьютеров.

Рассчитаем ожидаемую полезность КА ВПО *Petya* в период с мая 2017 г.:

$$EU_{\Sigma} = (1-\rho_n)U\left(W_m + W_j\right) + \rho_n U\left(W_m + W_j - F\right) =$$

$$= (1-0)\cdot \ln\left(\frac{2520000 - 46200 + 80000 + 6240}{6240}\right) -$$

$$0\cdot \ln\left(83\cdot\left(\frac{2520000 - 46200 + 80000 + 6240}{6240}\right)\right) = 6,02,$$

$$EU_A = (1-\rho_n)U\left(W_m + W_j\right) + \rho_n U\left(W_m + W_j - F\right)$$

$$= (1-0)\cdot \ln\left(\frac{2520000 - 46200 + 6240}{6240}\right) -$$

$$0\cdot \ln\left(83\cdot\left(\frac{2520000 - 46200 + 6240}{6240}\right)\right) = 5,98.$$

Тогда $\rho\left(\frac{EU}{A}\right) = \frac{EU_{нл}}{EU_{\Sigma}} = \frac{5,98}{6,02} = 0,99$.

Себестоимость КА ВПО *Petya* в соответствии с данными [35, 133-135] составила 46,2 тыс. руб. Таким образом, в период, начало которого датируется маем 2017 г.:

$$\alpha_j = \frac{\left(1-\rho_{nj}\right)\left(W_{mj} + W_j\right) + \rho_{nj}\left(W_{mj} + W_j - F_j\right)}{W_{mj} - C_j} =$$

$$\frac{(1-0)\cdot(80000 + 2520000) + 0\cdot(0 + 80000 + 2520000 - 84\cdot 80000)}{2520000 - 16200} = 1,05.$$

Рентабельность КА ВПО *Petya*, как обосновано в разделе 2.6.4, может быть оценена как $1/\alpha_j$, составила 95%. Зависимость вероятности использования ВПО *Petya* для реализации КА $Y(t) = \frac{1}{1-1,05e^{-212t}}$ представлена на графике 2-19.

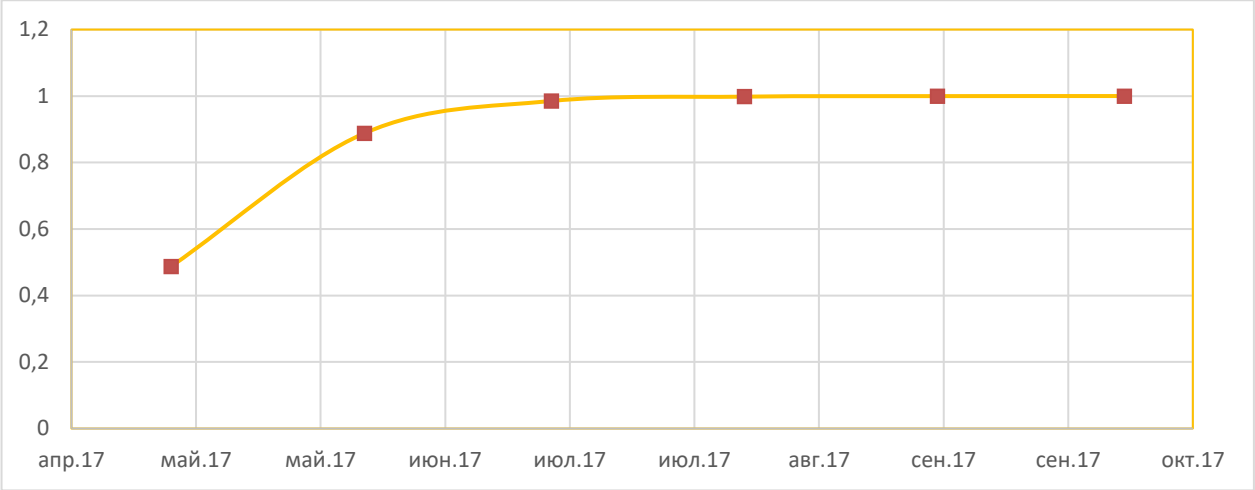

Рисунок 2-19. Зависимость вероятности использования ВПО *Petya* для реализации КА

Из рисунка 2.19 видно, что в июне $\rho_m(A)=0{,}89$, следовательно, повтор КА, аналогичной КА, реализованной с помощью ВПО *WannaCry*, была весьма высокой.

Из рисунков 2-17 – 2-19 также видно, что вероятность возможности использования КА ВПО *Petya* существенно возросла после успешного тестирования КА ВПО *Petya* в апреле 2016 г., а условная вероятность достаточности ожидаемой полезности использования КА ВПО *Petya* с точки зрения нарушителя, при оценивании которой учитывается возможность проведения незаметной КА, $p(EU\ A)=\rho\left(\frac{EU}{A}\right)p(A)\to 1$ после мая 2017 г.

Таким образом успешные КА, о которых информация появляется на сайтах новостных агрегаторов, приводит к появлению «подражателей» и повторению КА. В этой связи ключевым этапом для отслеживания новых методов КА является этап Теоретической подготовки, и, в первую очередь, фаза принятия решения о проведении КА, на котором отрабатывается практическая апробация метода КА. Анализ источников, которые позволяют выявлять факт апробации нового метода КА и реализовать мероприятия по его предотвращению, проводится в главе 3.

2.6.7. Итоги анализа математической модели развития компьютерной атаки

На основе ТДИ и натурного моделирования предложена и обоснована математическая модель, описывающая динамику КА, позволяющая определить вероятность возможности успешного проведения КА и параметров, от которых зависит эта вероятность.

Из проведенного анализа математической модели развития КА во времени можно сделать следующие выводы:

1. Вероятность выбора нарушителем вектора КА зависит от характеристик самой КА, но не от внешних характеристик, в частности, экономичности и рентабельности реализации метода КА, наличием рекламы в *DarkNet* и данными межличностного взаимодействия нарушителей и апробации (совместимости с инфраструктурой атакуемых организаций, простотой реализации, наличием средств ЗИ и методов обнаружения КА).

2. КА развивается по каскадной модели, динамика реализации каждого метода вектора реализуемой КА описывается *s*-образными кривыми Перла-Рида.

3. Этапы КА с точки зрения нарушителя разделяются на:

– теоретическую подготовку;

– практическую подготовку;

– достижение цели.

Существует возможность недопущения нанесения ущерба организации (снижение ожидаемой полезности от КА), а также увеличения вероятности и величины наказания нарушителя за счет выявления КА на первом и втором этапе ее реализации, что сокращает вероятность проведения КА.

В соответствии с ТДИ нарушителей можно классифицировать по признаку их индивидуальной предрасположенности к восприятию нового метода КА. Следовательно, выявив методы КА, реализуемые нарушителями-новаторами и их ранними последователями, можно предотвратить применение данного метода КА на большую часть узлов КС организации. Также отметим, что предварительное тестирование метода на втором этапе нарушитель может проводить не на целевой организации, поэтому целесообразно использовать данные систем сбора статистики со средств защиты КС центров мониторинга инцидентов ИБ для

анализа динамики развития возможности применения данного метода КА во времени на основе использования функции, описывающей динамику распространения инновации.

4. Нарушители предпочитают использовать известные методы КА, либо адаптировать и дорабатывать их под новую инфраструктуру, значительно чаще, чем разрабатывать новые векторы КА.

5. КА может быть технически прекращена нарушителем:

– если у него будет недостаточно навыков, методов и инструментов для КА, либо они не будут успешно реализовываться на любом из этапов КА;

– если КА будет обнаружена на этапе теоретической или практической подготовки.

6. КА может быть прекращена специалистом ИБ, если КА обнаружена и имеются средства ЗИ, которые позволяют заблокировать реализуемую КА.

7. Реализация КА может быть начата нарушителем, если:

– методы КА достаточно просты для реализации нарушителем;

– нарушителю известен метод КА;

– метод КА применим для инфраструктуры организации;

– в организации отсутствуют или недостаточны меры мониторинга защиты от данной КА.

8. КА на информационные ресурсы, не относящиеся к ценным активам для организации, может пройти, как показывает анализ фиксации обращений в правоохранительные органы по факту киберпреступлений, незамеченной, если не нарушены свойства критичной (защищаемой) организацией информации. Таким образом, предложенный подход по определению методов КА с точки зрения нарушителя позволит обеспечить полноту и актуальность реально используемых методов КА.

9. Выбор конкретного метода проведения КА определяется:

– наличием и известностью метода КА, в том числе в *DarkNet*;

– отсутствием мер защиты от КА;

– не реализуются мероприятия по мониторингу КА;

– совместимостью с широко распространенной инфраструктурой организаций;

– отсутствием видимого вреда для объекта КА.

2.7. Выводы

1. Разработаны математические модели принятия решения нарушителем о проведении КА и динамики изменения возможности использования КА во времени.

2. Ключевыми особенностями данных математических моделей, снимающими ограничения существующих методологий по формированию модели угроз и оценки рисков ИБ, являются:

– возможность учета динамики вероятных изменений векторов КА при расчете вероятности реализации КА;

– рассмотрение объекта КА и угрозы/риска ИБ с точки зрения нарушителя;

– возможность вычисления оценок ожидаемой полезности от КА и вероятности возможности успешной реализации КА.

3. Обоснован набор параметров математических моделей, использующихся для расчета вероятности реализации КА, и источников соответствующей информации, необходимой для вычисления соответствующих оценок.

Глава 3. Разработка методики прогнозирования динамики вероятности проведения компьютерной атаки, основанной на использовании предложенных математических моделей, и подтверждение ее работоспособности

Анализ результатов научных исследований, проведенный в разделе 1.3, показал, что в большинстве исследований оценка эффективности и практической применимости предлагаемых подходов и методов оценки угроз БИ и рисков ИБ не проводится. Практические примеры реализации, приводимые в работах [19, 34, 63, 66, 67], зачастую используют либо несвязанные с реальными данными значея переменных показателей, либо их экспертные оценки. В этой связи в данной главе разрабатывает методика прогнозирования вероятности угроз ИБ с точки зрения нарушителя, проводится анализ источников первичной статистической информации для проведения оценок для практической оценки, а также оценка адекватности данной методики.

Данная методика основана на установленной в главе 1 особенности реализации КА, проявляющейся в том, что вероятность проведения КА нарушителем является условной вероятностью достаточности ожидаемой полезности КА при наличии возможности реализации КА, которая вычисляется в соответствие с (2.1). При этом.

1. Оценки векторов возможных КА, для которых вычисляется оценка вероятности КА на организацию, могут быть получены на основе анализа данных *DarkNet*, так как нарушители предпочитают использовать известные методы КА, либо адаптировать и дорабатывать их под новую инфраструктуру, чем разрабатывать новые векторы КА.

2. Возможность реализации метода КА и вектора КА можно оценить в соответствие с (2.21) и (2.22).

3. Оценку достаточности ожидаемой полезности КА можно вычислить в соответствие с (2.2) и далее использовать ее для расчета вероятности принятия решения о проведении КА для всего перечня векторов КА.

4. Оценку условной вероятности достаточности ожидаемой полезности КА с точки зрения нарушителя, в которой учитывается возможность проведения незаметной КА, можно рассчитывать по формуле (2.1). При этом для нахождения оценок значений параметров функций (2.2), (2.21), (2.22) достаточно использовать информацию из общедоступных источников, выбор и релевантность которых обосновываются в данной главе.

3.1. Анализ общедоступных источников информации о компьютерных атаках с точки зрения достаточности хранимой в них информации для идентификации параметров разработанных математических моделей компьютерной атаки и оценки их адекватности

Статистические данные о КА, собираются как исследователями, так и коммерческими и государственными организациями, в том числе из сети *DarkNet* [35, 122, 134]. В РФ большую работу по сбору статистики об инцидентах ИБ ведет Центральный банк России [106, 107, 108]. В РФ в соответствии с Указом Президента РФ № 31с от 15.01.2013 [136] создана государственная система обнаружения, предупреждения и ликвидации последствий КА (ГосСОПКА) для централизованного сбора информации об инцидентах ИБ в РФ. В настоящее время активно прорабатываются вопросы, связанные с анализом данных, собираемых системой ГосСОПКА. Это подтверждается формулировкой одной из задач направления ИБ цифровой экономики РФ: «повышение уровня автоматизации процессов принятия решений и уменьшить время реакции на инциденты ИБ при использовании в корпоративных и отраслевых центрах ГосСОПКА» [89]. Также ведут сбор статистических данных корпоративные центры мониторинга и производители средств защиты, которые публикуют соответствующие отчеты. Общедоступные источники информации для оценки эффективности и реалистичности математической модели, описанной в главе 2, приведены в приложении А.

Из анализа общедоступных источников [35, 104, 105, 122, 134, 137-167] видно, что статистические данные об КА можно разделить на следующие группы:

– данные, собранные исследовательскими институтами и лабораториями, занимающимися анализом данных из *DarkNet* [35, 122, 134];

– данные, собранные центрами мониторинга ИБ; данные собранные производителями средств защиты информации;

– данные, собранные новостными агрегаторами.

Отметим, что анализ форумов в *DarkNet* позволяет собрать информацию о стратегиях, тактиках и методах, которые используют и/или разрабатывают нарушители [35, 122, 134]. Также в [122] рассмотрены решения по сбору информации из онлайн чатов *IRC* и магазинов по распространению метаданных с пластиковых карт (*carding shops*). Здесь для представления, полученных данных, к единому виду, анализу и последующей обработке используются различные механизмы машинного изучения: классификатор случайного леса, случайного дерева и наивный байесовский классификатор [134]. Однако разработка автоматизированных методов анализа информации, извлеченной из *DarkNet*, а также интеллектуальных баз знаний угроз (*Cyber Threat Intelligence*), находится в настоящее время только на начальной стадии.

Анализ результатов исследований *DarkNet* показывают, что на форумах *DarkNet*, в первую очередь, обсуждаются эксплоиты и утилиты, которые используются для реализации КА. Среди наиболее обсуждаемых утилит – ПО для создания вирусов, которые могут обходить системы ИБ, ПО для подбора паролей и удаленного администрирования. Наибольшее число эксплоитов, упоминаемых на форумах *DarkNet* относится к безопасности сетевой инфраструктуры и ОС, около 15% – к веб-приложениям и мобильным технологиям [122]. Отметим, что нам не удалось обнаружить работ, в которых описаны методы использования информации, извлеченной из *DarkNet*, для проектирования векторов КА.

Сегмент центров мониторинга ИБ включает в себя как государственный, так и коммерческие центры мониторинга и сервис провайдеров услуг ИБ различных стран. Однако данные центры, как правило, предоставляют не полную информацию, так как раскрытие всего объема информации в публичном доступе

может привести к дополнительной осведомленности нарушителя. Например, в отчете Финцерта [106–108, 113] предоставлена подробная информация по различным угрозам для организаций финансового сектора за исключением нанесенного ущерба каждой из угроз. Также отметим достаточно подробный отчет организации «*PURPLESEC*» [138], который содержит статистику не только по угрозам, но и по сферам человеческой деятельности, подвергавшихся КА.

Анализ данных отчетов позволяет извлечь полезную информацию о векторах КА. Например, по данным *NTT Ltd. Global Threat Intelligence Report* за 2020 г. [152] 33% от общего числа обнаруженных КА атак во всем мире были связаны с приложениями, а 22% – с веб-приложениями. Это означает, что в общей сложности 55% атак, обнаруженных во всем мире, происходили на уровне приложений. По данным *Gartner Group* [168], расходы на сегмент рынка ИБ в течение 2020 г. составили около 133,776 миллионов долларов США в год. При этом около 3,3 миллиона долларов из этой суммы были затрачены на решение проблем, связанных с ИБ приложений (около 2,4%).

Отметим, что статистические отчеты сегмента производителей средств ЗИ, как правило, не содержат информации об объемах статистических данных, которые были проанализированы для оценки вектора КА, оценивании ущерба, нанесенном организации инцидентом ИБ, и прибыли, полученной злоумышленником от реализации КА. Здесь исключение представляют отчеты фирмы *Symantec* [142], в которых указывается объем проанализированных статистических данных.

Сегмент новостных агрегаторов содержит информацию о размерах ущерба от инцидентов ИБ и заработке нарушителей. Однако эти данные не являются полными, так как они не охватывают весь объем успешно реализованных КА, но оказываются единственным источником о заработке нарушителя ИБ. Отметим, что нарушитель не обладает исходными данными о ценности данных в той или иной организации, однако, он может использовать информацию, размещаемую новостными агрегаторами, для подготовки и реализации КА, затрагивающих

максимально возможное количество организаций, ориентироваться на данные бухгалтерской отчетности.

Таким образом, единого универсального источника информации о реализованных КА сегодня не существует, поэтому в качестве источника исходных данных при прогнозировании вероятности КА целесообразно использовать данные из *DarkNet,* отчеты центров мониторинга инцидентов ИБ, а также информацию, предоставляемую новостными агрегаторами и доступную бухгалтерскую отчетность.

3.2. Модель нарушителя и ее влияние на компьютерную атаку

В соответствии с нормативными документами ФСТЭК [5, 6] и ФСБ России [8] при формировании модели угроз необходимо разрабатывать модель нарушителя, что подробно расписано в главе 1.

Следуя [5], будем использовать следующую классификацию нарушителей, осуществляющих КА в сети Интернет:

– специальные службы иностранных государств;

– отдельные физические лица («хакеры»);

– конкурирующие организации.

Так как порядок этапов проведения КА не зависит от типа нарушителя, то можно использовать предложенную методологию для всех типов нарушителей, при необходимости, корректируя источники общедоступной информации.

Для подтверждения, данного утверждения, рассмотрим два крайних случая:

– нарушителя, не обладающего знаниями в области ИТ и ИБ (например, школьника или пенсионера);

– нарушителя, обладающего неограниченными ресурсами и возможностями получать знания (например, сотрудника специальной службы иностранного государства).

Нарушитель, не обладающий знаниями в области ИТ и ИБ

К данному типу нарушителей можно отнести, например, школьников и студентов младших курсов. Отличительной особенностью данного типа является не знание законодательства РФ, а также отсутствие легального текущего дохода. Поэтому в (2.2), (2.28) достаточно подставить следующие значения $F_j=0$, $W_j = 0$.

Нарушитель, обладающий неограниченным ресурсам и возможностями получать знания

К данному типу нарушителей следует отнести специальные службы иностранных государств. При определении ожидаемой полезности необходимо учитывать, что величина тяжести наказания F_j зависит не от Уголовного кодекса РФ, но от тяжести последствий для иностранного государства при выявлении его причастности к подобной деятельности. В связи с этим, можно сделать вывод, что для сокрытия своего типа нарушитель будет стараться использовать данные, как и любой другой нарушитель, т.е. методы *DarkNet*.

Это подтверждает и статистика по оценкам [32], количество совершенно нового ВПО, появившегося в период с 3 квартала 2016 г. по 2 квартал 2018 г., составило менее 10% от общего числа ВПО. Так как для реализации КА используется несколько методов КА (см. главу 2), то в части этапов реализации КА данным типом нарушителя будут использоваться методы из общедоступных источников информации. Подтверждением данному высказыванию служит то, что многие специалисты считают КА ВПО *Petya*, реализованной специальными службами.

Таким образом, при прогнозировании вектора КА необходимо определить модель нарушителя, на основании которой необходимо выбирать наиболее подходящие общедоступные источники информации. Сама методология оценивания вероятностей КА при этом не изменится.

3.3. Методика оценивания параметров функции прогнозирования динамики компьютерной атаки

Прогнозирование динамики развития КА реализуется на этапе теоретической и практической подготовки с точки зрения нарушителя. Расчет вероятности $P(EUA) = P(EU|A)P(A)$ реализуется выполнением следующей последовательности действий.

1. Расчет параметров ожидаемой полезности

1.1. Оценка КА на основе анализа доступных источников информации об успешных КА, количества выявленных КА данного типа A_m.

1.2. Оценка КА на основе анализа доступных источников информации об успешных КА, количества выявленных КА, закончившихся обращением пострадавших в правоохранительные органы и/или арестом (наказанием преступника) A_{mf}.

1.3. Вычисление вероятности проведения незаметной КА $\rho_m = \frac{A_m - A_{mf}}{A_m}$.

1.4. Вычисление вероятности разоблачения нарушителя $\rho_n = 1 - \rho_m$.

1.5. Оценка выручки нарушителя в случае успешной реализации КА $W_{mpj}^{\langle сум \rangle}$, на основе использования информации о выгоде, полученной нарушителем в ходе успешных реализаций аналогичных методов КА, из общедоступных источников (например, таблица 2-1) с учетом количества КА данного типа, реализуемых нарушителем одновременно.

1.6. Оценка стоимости проведения КА, используя общедоступные источники информации о КА в сетях *DarkNet* C_j (например, используя приложение F).

1.7. Вычисление прибыли нарушителя в случае успешной реализации КА $W_{mj} = W_{mpj}^{\langle сум \rangle} - C_j$.

1.8. Оценка текущего дохода нарушителя от легальной деятельности, используя зависимость, представленную на рисунке 2-1.

1.9. Определение, используя таблицу 2-2, тяжести наказания в случае разоблачения нарушителя F_j.

1.10. Определение параметров функции $U(\xi) = b\ln\left(\frac{a+\xi}{a}\right)$, a – МРОТ за рассматриваемый период времени, b =1.

1.11. Вычисление ожидаемой полезности от КА по формуле:

$$EU_{нл} = (1-\rho_n)U(W_m) + \rho_n U(W_m - F_j).$$

1.12. Вычисление ожидаемой полезности от КА с учетом всех доходов ожидаемой полезности от легальной деятельности по формуле:

$$EU_{\Sigma} = \sum_{j=1}^{J} EU_j$$

1.13. Вычисление условной вероятности достаточности ожидаемой полезности $P(EU|A)$ по формуле:

$$P(EU|A) = \frac{EU_{нл}}{EU_{\Sigma}}$$

2. Расчет параметров возможности реализации метода КА

2.1. Оценка на основе исполования доступных источников информации об успешных КА, количества попыток реализации КА данного типа A_l.

2.2. Оценка на основе исполования доступных источников информации об успешных КА, количества успешно реализованных КА A_{lp}.

2.3. Вычисление коэффициентов межличностной рекламы метода КА (успешности реализации аналогичных КА) $a_l = \frac{A_{lp}}{A_l}$.

2.4. Оценка на основе исполования доступных источников информации об успешных КА, количества попыток апробации КА данного типа A_p.

2.5. Оценка на основе исполования доступных источников информации об успешных КА, количества успешно реализованных апробаций КА (логи центров мониторинга ИБ A_{pp}).

2.6. Вычисление коэффициента апробации метода КА в *DarkNet* (успешная практическая проверка метода КА), оцениваемый на основе данных новостных агрегаторов и/или данных центров мониторинга ИБ $a_p = \frac{A_{pp}}{A_p}$.

2.7. Вычисление коэффициента известности метода КА в *DarkNet* a_n (например, используя приложение F).

2.8. Вычисление параметра $\beta = a_n + a_l + a_p$.

2.9. Вычисление параметра $\alpha_j = \frac{\left(1-\rho_{nj}\right)\left(W_{mpj}+W_j\right)+\rho_{nj}\left(W_{mpj}+W_j-F_j\right)}{W_{mpj}-C_j}$

2.10. Вычисление вероятности возможности реализации выбранного метода КА $P(A,t) = \frac{1}{1+\alpha_j e^{-\beta_j t}}$.

3.4. Пример практического использования методики прогнозирования динамики компьютерной атаки, основанной на использовании предложенных математических моделей

Проведем прогнозирование тренда КА на КФС на 2019 г., перечень КА для анализа представлен ниже:

- целевые атаки на организации КФС;
- нецелевые (спам-атаки) на организации КФС;
- нецелевые атаки на клиентов КФС через зараженные популярные сайты;
- нецелевые атаки на клиентов КФС с использованием ВПО;
- нецелевые атаки на клиентов с использованием социальной инженерии.

Для это будем использовать статистику Центрального банка за 2017, 2018, 2019 годы [106-108], а также данные новостных агрегаторов о КФС [104]. В качестве нарушителя рассмотрим нарушителя, имеющего доступ в *DarkNet*, но при этом не обладающего неограниченным ресурсом. Для оценки известности метода КА будем использовать статистику *DarkNet* (Приложение F), для оценки

заработной платы – легальной выгоды, воспользуемся данными с сайта *Superjob* [115].

1. ***Расчет условной вероятности достаточности ожидаемой полезности для КА на КФС за 2017, 2018 гг.***

1.1. Оцениваем, используя [104-108], количество выявленных КА данного типа A_m в 2017 и 2018 гг., значение числа которое приведено в таблице 3-1, соответственно. (п. 1.1 Методики).

1.2. Оцениваем, используя [104-108], количество выявленных КА данного типа, закончившихся обращением пострадавших в правоохранительные органы и/или арестом (наказанием преступника) A_{mf} в 2017 и 2018 гг. , значение числа которое приведено в таблице 3-1, соответственно. (п. 1.2 Методики).

1.3. Вычисляем вероятность проведения незаметной КА $\rho_m = \frac{A_m - A_{mf}}{A_m}$. (п. 1.3 Методики). Результаты расчетов представлены в таблице 3-1 за 2017, 2018 гг.

Таблица 3-1. Вероятность проведения КА незаметной за 2017, 2018 гг.

j	Наименование КА	2017 г.			2018 г.		
		ρ_m	A_m	A_{mf}	ρ_m	A_m	A_{mf}
1	Целевые КА на организации КФС	0,949	39	2	0,945	72	4
2	Нецелевые (спам-атаки) на организации КФС	1	200000	0	1	300000	0
3	Нецелевые КА на клиентов КФС через зараженные популярные сайты	1	481	0	1	2205	0
4	Нецелевые КА на клиентов КФС с использованием ВПО	1	63582	0	0,999	1029438	2
5	Нецелевые КА на клиентов с использованием социальной инженерии	0,999	27567	1	1	36000	0

1.4. Вычисляем вероятность разоблачения нарушителя p_n. (п. 1.4 Методики). Результаты расчетов для перечня КА представлены в таблицах 3-3 и 3-4 за 2017, 2018 гг., соответственно.

1.5. Оцениваем выручку нарушителя в случае успешной реализации КА $W_{mpj}сум$, используя информацию о выгоде полученной нарушителем в ходе успешных реализаций аналогичных методов КА, приведенную в таблице 2-1 с учетом количества КА данного типа, реализуемых нарушителем одновременно. (п. 1.5 Методики). (Результаты расчетов представлены в таблице 3-2 за 2017, 2018 гг., соответственно.)

1.6. Определяем стоимости реализации КА в сетях *DarkNet* C_j из приложения F. (п. 1.6 Методики). (Результаты расчетов представлены в таблице 3-2 за 2017, 2018 гг., соответственно.)

1.7. Вычисляем прибыль нарушителя в случае успешной реализации КА $W_{mj} = W_{mpj}сум - C_j$. (п. 1.7 Методики). (Результаты расчетов представлены в таблице 3-2 за 2017, 2018 гг., соответственно.)

Таблица 3-2. Прибыль нарушителя в случае успешной реализации КА

j	Наименование КА	2017 г.			2018 г.		
		W_{mj}	$W_{mpj}сум$	C_j	W_{mj}	$W_{mpj}сум$	C_j
1	Целевые КА на организации КФС	48789200	49034000	244800	3579200	3824000	244800
2	Нецелевые (спам-атаки) на организации КФС	313978400	314000000	21600	1569978400	1570000000	21600
3	Нецелевые КА на клиентов КФС через зараженные популярные сайты	5240000	5280000	40000	24160000	24200000	40000
4	Нецелевые КА на клиентов КФС с использованием ВПО	99799000	99820600	21600	1616183500	1616205100	21600
5	Нецелевые КА на клиентов с использованием социальной инженерии	30591200	30591600	400	399599600	399600000	400

1.8. Оцениваем текущий доход нарушителя от легальной деятельности, используя зависимость, представленную на 2-1. (п. 1.8 Методики): в 2017 г. – w_j=80000, в 2018 г. w_j=83000.

1.9. Определяем, используя 2-2, тяжесть наказания в случае разоблачения нарушителя F_j. (п. 1.9 Методики). (Результаты представлены в таблицах 3-3 и 3-4 за 2017, 2018 гг., соответственно.)

1.10. Определяем параметры функции (п. 1.10 Методики): a = 11 163 руб. в 2018 г., a = 7 800 руб. в 2017 г., b =1.

1.11. Вычисляем ожидаемую полезность от КА $EU_{\text{нл}}$. (п. 1.11 Методики). Результаты представлены в таблицах 3-3 и 3-4 за 2017, 2018 гг., соответственно.

1.12. Вычисляем ожидаемую полезность от КА с учетом всех доходов, учитывая ожидаемую полезность от легальной деятельности $EU_{\Sigma} = \sum_{j=1}^{J} EU_j$. (п. 1.12 Методики): $EU_{\Sigma} = 48{,}918$ в 2018 г., $EU_{\Sigma} = 42{,}809$ в 2017 г.

1.13. Вычисляем условную вероятность достаточности ожидаемой полезности $\rho\left(\frac{EU}{A}\right)$. (п. 1.13 Методики). (Результаты представлены в таблицах 3-3 и 3-4 за 2017, 2018 гг., соответственно.)

Таблица 3-3. Расчет условной вероятности достаточности ожидаемой полезности в КФС КА в 2017 г.

j	Наименование КА	$P(EU\|A)$	$EU_{\text{нл}}$	F_j	ρ_n
1	Целевые КА на организации КФС	0,170	7,297	4076462000	0,051
2	Нецелевые (спам-атаки) на организации КФС	0,239	10,245	26068640000	0
3	Нецелевые КА на клиентов КФС через зараженные популярные сайты	0,144	6,154	444880000	0
4	Нецелевые КА на клиентов КФС с использованием ВПО	0,213	9,098	8291749800	0
5	Нецелевые КА на клиентов с использованием социальной инженерии	0,185	7,915	2545742800	0,000

Из таблицы 3-3 видно, что фокус внимания нарушителей сосредоточен на организациях КФС, нежели, чем на их клиентах. Это связано, с тем, что КА на КФС позволяет получить большую прибыль.

Ожидаемая полезность у целевых КА ниже чем у нецелевых КА, несмотря на большую прибыль нарушителя от реализации целевой КА, это связано с тем, что в 2017 г. было арестовано 2 группы нарушителей, реализующих целевые КА. При этом ожидаемая полезность от целевой КА существенно велика. Это говорит, о том, что выгода от нелегальной деятельности при реализации целевых КА существенно больше нежели, чем любой другой способ заработка для нарушителя.

Вероятность разоблачения нарушителя для нецелевых КА равна нулю. Это объясняется тем, что нецелевая КА на один объект приносит примерно одинаковую выгоду (менее 16 тыс. руб.). В связи с тем, что величина этой выгоды для организаций существенно мала, даже по сравнению с заработной платой юриста, которого необходимо привлечь для доведения правонарушения, связанного с нецелевой КА до суда, то вероятность разоблачения нарушителя $\rho_n = 0$. Такие результаты позволяют сделать вывод, что количества попыток реализации нецелевых КА будет расти в следующие периоды, новые методы реализации нецелевых КА будут активно разрабатываться. Кроме того, для снижения вероятности разоблачения нарушителя p_n при целевых КА нарушители могут попробовать снизить выручку от реализации целевой КА на одну организацию, чтобы снизить число обращений в правоохранительные органы.

Таблица 3-4. Расчет условной вероятности достаточности ожидаемой полезности в КФС КА в 2018

j	Наименование КА	$P(EU\|A)$	$EU_{\text{нл}}$	F_j	ρ_n
1	Целевые КА на организации КФС	0,099	4,882	324281000	0,056
2	Нецелевые (спам-атаки) на организации КФС	0,242	11,854	130317000000	0
3	Нецелевые КА на клиентов КФС через зараженные популярные сайты	0,157	7,680	2015489000	0
4	Нецелевые КА на клиентов КФС с использованием ВПО	0,243	11,883	134152000000	0

5	Нецелевые КА на клиентов с использованием социальной инженерии	0,214	10,486	33173689000	0

Из таблицы 3-4 видно, что предпосылки, сформулированные из анализа результатов, полученных из расчетов по данной методике за 2017 г., приведенных в таблице 3-3, подтвердились. Увеличение количества арестов за целевые КА привело к существенному снижению выручки от реализации целевой КА на одну организацию. Соответственно, снизилась условная вероятность достаточности ожидаемой полезности от целевой КА. Ожидаемая полезность от реализации нецелевых КА, как и предполагалось возросла. Минимальная ожидаемая полезность среди нецелевых КА у нецелевых КА на клиентов КФС через зараженные популярные сайты. Это связано с тем, что к группе взаимодействия ФинЦерт подключились операторы связи и наладился процесс блокировки зараженных сайтов, что сократило количество КА. Хотелось бы отдельно отметить, что вероятность разоблачения нарушителя $\rho_n = 0$ для нецелевых КА на клиентов КФС через зараженные популярные сайты в связи с тем, что наказания злоумышленников не последовало (не было уголовных и административных дел).

2. Расчет вероятности возможности реализации КА на КФС за 2017, 2018 гг.

2.1. Оцениваем, используя доступные источники об успешных КА, количество попыток реализации КА данного типа A_l. (п. 2.1 Методики). (Результаты за 2017, 2018 гг. приведены в таблицах *3-5* и *3-6*, соответственно.)

2.2. Оцениваем, используя доступные источники об успешных КА, количество успешно реализованных КА A_{lp}. (п. 2.2 Методики). (Результаты за 2017, 2018 гг. приведены в таблицах *3-5* и *3-6*, соответственно.)

2.3. Вычисляем коэффициент межличностной рекламы метода КА (успешности реализации аналогичных КА) $a_l = \frac{A_{lp}}{A_l}$. (п. 2.3 Методики).

(Результаты за 2017, 2018 гг. приведен в таблицах *3-5* и *3-6*, соответственно.)

2.4. Так как проведенный анализ общедоступных источников об успешных КА, не выявил данных о попытках апробации КА данного типа $A_p = 0$. (п. 2.4 Методики).

2.5. Так как анализ общедоступных источников об успешных КА, не выявил успешно реализованных апробациях КА $A_{pp} = 0$. (п. 2.5 Методики).

2.6. Вычисляем коэффициент апробации метода КА в *DarkNet*: $a_p = \frac{A_{pp}}{A_p} = 0$ для всех рассматриваемых методов КА. (п. 2.6 Методики).

2.7. Вычисляем коэффициенты известности метода КА в *DarkNet* a_n, используя приложение F. (п. 2.7 Методики). (Результаты за 2017, 2018 гг. приведен в таблицах *3-5* и *3-6*, соответственно.)

2.8. Вычисляем параметр $\beta = a_n + a_l + a_p$. для рассматриваемого перечня КА. (п. 2.8 Методики). (Результаты за 2017, 2018 гг. приведен в таблицах *3-5* и *3-6*, соответственно.)

2.9. Вычисляем параметр α_j для рассматриваемого перечня КА. (п. 2.9 Методики). (Результаты за 2017, 2018 гг. приведен в таблицах *3-5* и *3-6*, соответственно.)

2.10. Вычисляем вероятность возможности реализации метода КА $p(A)$. (п. 2.10 Методики). (Результаты за 2017, 2018 гг. приведен в таблицах *3-5* и *3-6*, соответственно.)

Расчёт вероятности возможности реализации КА за 2017, 2018 гг. приведен в таблицах *3-5* и *3-6*, соответственно.

Таблица 3-5. Возможность реализации КА в КФС за 2017 г.

j	Наименование КА	$P(A)$	α_j	β	a_n	a_l	A_{lp}	A_l
1	Целевые КА на организации КФС	0	-3,278	122,872	0,28	0,949	37	39
2	Нецелевые (спам-атаки) на организации КФС	0,499	1,000	112	0,12	1	200000	200000

3	Нецелевые КА на клиентов КФС через зараженные популярные сайты	0,494	1,023	140	0,4	1	481	481
4	Нецелевые КА на клиентов КФС с использованием ВПО	0,499	1,001	112	0,12	1	63582	63582
5	Нецелевые КА на клиентов с использованием социальной инженерии	0,500	0,999	129,996	0,3	0,999	27566	27567

Из таблицы 3-5 видно, что рентабельность целевых КА на КФС может быть оценена как $1/\alpha_j$, что обосновано в разделе 2.6.4, и отрицательна. Таким образом, реализация целевых КА на КФС в том виде, что они были в 2017 году в последующие годы не возможна $p(A)=0$. Расчеты также показывают, что наиболее активно развиваются КА с использованием социальной инженерии. Это объясняется тем, что данный тип КА зачастую требует минимальных знаний в ИТ и ИБ сфере, используя стандартные мошеннические механизмы правонарушителей для получения конфиденциальной информации, тем самым увеличивая число нарушителей, использующих данный тип КА.

Таблица 3-6. Возможность реализации КА в КФС за 2018 г.

j	Наименование КА	$P(A)$	α_j	β	a_n	a_l	A_{lp}	A_l
1	Целевые КА на организации КФС	0	-3,941833681	122,44	0,28	0,949	68	72
2	Нецелевые (спам-атаки) на организации КФС	0,499	1,00	112	0,12	1	300000	300000
3	Нецелевые КА на клиентов КФС через зараженные популярные сайты	0,498	1,01	140	0,4	1	2205	2205
4	Нецелевые КА на клиентов КФС с использованием ВПО	0,500	0,999	111,99	0,12	1	1029436	1029438
5	Нецелевые КА на клиентов с использованием социальной инженерии	0,500	1,00	130	0,3	0,999	36000	36000

Из таблицы 3-6 видно, что действительно тип целевых КА на КФС существенно изменился: средняя сумма выручки нарушителя сократилась в 12 раз, так как возросло число попыток замаскировать целевую КА. Однако, видоизменение целевой КА не помогло, так как число уголовных дел в отношении нарушителей, реализовывающих целевые КА на КФС, увеличилось.

Логично предположить, что целевые КА на КФС продолжат видоизменяться. В том, числе путем изменения фокуса с КФС на клиентов КФС, о чем свидетельствует увеличение вероятности возможности реализации нецелевых КА на клиентов КФС с использованием ВПО.

Возможность реализации КА с использованием социальной инженерии стабильно высока, что говорит, об активном распространении метода КА среди нарушителей. Это объясняется тем, что одни и те же методы социальной инженерии можно неоднократно применять, так как объектом КА зачастую является человек (в случае с другими КА из списка можно использовать специальные автоматические средства ЗИ, у которых возможно оперативно и централизовано поменять конфигурацию).

3. Анализ прогноза на 2019 год

Вероятность ожидаемой полезности при условии возможности реализации КА в 2017 и 2018 гг., а также прогнозное значение вероятности ожидаемой полезности при условии возможности реализации КА за 2019 г. представлены в таблице 3-7.

Таблица 3-7. Вероятность ожидаемой полезности за 2017, 2018, 2019 гг.

j	Наименование КА	*P*(*EUA*) в 2017 г.	*P*(*EUA*) в 2018 г.	*P*(*EUA*) в 2019 г.
1	Целевые КА на организации КФС	0	0	0
2	Нецелевые (спам-атаки) на организации КФС	0,120	0,121	0,122
3	Нецелевые КА на клиентов КФС через зараженные популярные сайты	0,071	0,078	0,085
4	Нецелевые КА на клиентов КФС с использованием ВПО	0,106	0,121	0,136
5	Нецелевые КА на клиентов с использованием социальной инженерии	0,092	0,107	0,122

Данные, представленные в таблице 3-7, позволили дать следующий прогноз трендов КА на 2019 г.

1. Целевые КА на организации КФС в том виде, в котором они реализовывались в 2017 и 2018 гг. в 2019 г. реализовываться не будут, так как вероятность ожидаемой полезности при наличии возможности реализации КА данного вида равна нулю. Это означает, что группы злоумышленников будут

видоизменять целевые КА (выгода с реализации КА, метод и т.п.), либо будут переходить на нецелевые КА.

2. Увеличится вероятность реализации нецелевых КА на клиентов КФС Об этом свидетельствует смещение фокуса внимания нарушителей с КФС на иные сферы бизнеса, так как КФС сумел построить единую централизованную систему оповещения о новых методах КА и оперативного предупреждения инцидентов ИБ, в том числе блокировки КА на уровне операторов связи. В сфере КФС сформировалась практика обращения в правоохранительные органы и доведения дел до суда, чего не скажешь про иные сферы бизнеса.

3. Минимальное значение вероятности нецелевых КА со сравнению с другими КА из таблицы 3-7 на клиентов КФС через зараженные популярные сайты по сравнению с другими нецелевыми КА. Это объясняется наличием механизма блокировки КА на уровне операторов связи.

4. Увеличится вероятность реализации нецелевых атак на клиентов КФС с использованием ВПО. Увеличение вероятность КА данного типа может быть связано, с тем, что данные КА технологически похожи на целевые КА, при этом они с точки зрения нарушителя не обладают ограничениями целевых КА.

5. Увеличится вероятность реализации нецелевых атак на клиентов с использованием социальной инженерии. Это объясняется тем, что данный тип КА зачастую требует минимальных знаний в ИТ и ИБ сфере, используя стандартные мошеннические механизмы правонарушителей для получения конфиденциальной информации, тем самым увеличивая число нарушителей, использующих данный тип КА. Одни и те же методы социальной инженерии можно неоднократно применять (рентабельность КА возрастает), так как объектом КА зачастую является человек (в случае с другими КА из списка можно использовать специальные автоматические средства ЗИ, у которых возможно оперативно и централизовано поменять конфигурацию).

В связи с тем, что в отчете Банка России [108, 113] не представлены количественные значения показателей КА за 2019 г., но только качественные описания фактических векторов КА, проведем сравнение спрогнозированной в

динамики изменений вероятности КА с аналогичными данными, представленными в отчете.

Результаты сравнения показывают, что прогноз динамики изменения векторов КА оказался верным по:

– целевым КА на организации КФС;

– нецелевым (спам-атаки) КА на организации КФС;

– нецелевым КА на клиентов КФС через зараженные популярные сайты;

– нецелевым КА на клиентов КФС с использованием ВПО;

– нецелевым атакам на клиентов с использованием социальной инженерии.

В 2019 г. по данным отчета Банка России:

1. Наблюдалось снижение количества попыток КА на организации КФС. Произошло смещение фокуса внимания злоумышленников с организаций кредитно-финансового сектора на их клиентов. В частности, сохранялась высокая интенсивность распространения нарушителями ВПО класса *ransomware* (целевых КА), но уже не на КФС.

2. Одним из основных инструментов компьютерных преступников, по-прежнему, оставалось ВПО.

3. В 2019 г. в арсенале злоумышленников появился новый способ обмана жертв – подмена исходящего телефонного номера на номер КФС и выдача себя за сотрудника безопасности банка.

4. У Банка России появились полномочия по инициированию снятия с делегирования мошеннических интернет ресурсов и построен процесс взаимодействия со всеми участниками процесса разделегирования. (Минимальное время разделегирования доменов фишинговых ресурсов составило 3 часа 3 дня, что стало возможным благодаря появлению дежурной службы, работающий в режиме 24/7/365.)

5. Был осуществлен переход 66% мошеннических ресурсов в юриспруденцию иностранных доменных зон. Что говорит об изменении тренда с нецелевых атак на клиентов КФС через зараженные популярные российские

сайты, на западные сайты. (Отметим, что у Банка России нет компетенций на разделегирования фишинговых ресурсов за пределами доменных зон *.ru*, .рф, *.su*).

Таким образом, прогноз динамики КА в 2019 г. оказался не противоречащим соответствующим данным Банка России, что подтверждает работоспособность предложенной методики прогнозирования вектора КА.

3.5. Выводы

1. Разработана методика прогнозирования векторов КА, позволяющая выявлять тренды развития КА с точки зрения нарушителя.

2. Проведен анализ источников общедоступной информации, позволяющий сделать вывод, о том что единого универсального источника информации о реализованных КА сегодня не существует, поэтому в качестве источника исходных данных при прогнозировании вероятности КА целесообразно использовать данные из *DarkNet*, отчеты центров мониторинга инцидентов ИБ, а также информацию, предоставляемую новостными агрегаторами и доступную бухгалтерскую отчетность.

3. Оценка результатов практической апробации подтвердила, что вектор КА определяется:

3.1. Вероятностью разоблачения нарушителя (вероятность проведения незаметной КА) для нарушителя, склонного к риску, и тяжестью наказания, для нарушителя, не склонного к риску. Осуществление защиты от КА возможно за счет изменения восприятия преступником возможностей (в том числе, соотношения между выгодой и потерями) совершения преступления путем повышения возможности разоблачения нарушителя.

3.2. Характеристиками самой КА, в частности, экономичностью и рентабельностью реализации метода КА, наличием рекламы в *DarkNet* и данными межличностного взаимодействия нарушителей и апробации (совместимости с инфраструктурой атакуемых организаций, простотой реализации, наличием средств ЗИ и методов обнаружения КА).

3.3. На текущий момент доходы от легальной деятельности существенно ниже выручки нарушителя от реализации КА.

ЗАКЛЮЧЕНИЕ

1. Проведен анализ состояния предметной области, в том числе, нормативно-правовой базы РФ, международных стандартов и ГОСТов по ИБ, а также научных исследований результаты, которого свидетельствует о наличии принципиальных ограничений существующих подходов по оценки угроз и рисков ИБ, связанных с отсутствием в данных подходах собственно нарушителя, реализующего КА.

2. Обоснованы базовые принципы и подходы, на которых построены с точки зрения нарушителя математическая модель принятия решения нарушителем о проведении КА и математическая модель, описывающей динамику изменения вектора КА во времени.

3. Разработана методика прогнозирования динамики изменения вектора КА, основанная на использовании предложенных математических моделей, и подтверждена ее работоспособность на основе использования данных об известных КА за 2017-2019 гг.

Перспективы дальнейшей разработки темы исследования заключаются в:

1. Определении значений параметров функции вероятности возможности реализации КА во времени на Практическом этапе и этапе Достижения цели.

2. Автоматизации сбора и анализа информации из общедоступных источников информации о КА для прогнозирования векторов КА во времени с точки зрения нарушителя.

3. Автоматизации процесса прогнозирования динамики изменения вектора КА с точки зрения нарушителя.

Список сокращений

АСУ ТП	автоматизированных систем управления технологическим процессом
БИ	безопасность информации
ВКП	весовой коэффициент перехода
ВПО	вредоносное программное обеспечение
ГИС	государственная информационная система
ГосСОПКА	государственная система обнаружения, предупреждения и ликвидации последствий компьютерной атаки
Д	доступность
ЗИ	защита информации
ИБ	информационная безопасность
ИС	информационная система
ИСПД	информационная система персональных данных
ИТ	информационные технологии
К	конфиденциальность
КА	компьютерная атака
КЗ	класс защищенности
КС	компьютерных сетях
КИИ	критическая информационная инфраструктура
КФС	кредитно-финансовый сектор
Методика	Методика определения угроз безопасности информации
МРОТ	Минимальный размер оплаты труда в Российской Федерации
МУ	модель угроз
ОС	операционная система
ПАК «*Ampire*»	программно-аппаратным комплексом обучения методам обнаружения, анализа и устранения последствий компьютерных атак «*Ampire*»
ПД	персональные данные
ПО	программное обеспечение
Системы и сети	ИС, автоматизированных системах управления, информационно-телекоммуникационных сетях, информационно-телекоммуникационных инфраструктурах центров обработки данных и облачных инфраструктурах
РФ	Российская Федерация
ст.	статья
СУИБ	система управления информационной безопасностью

ТДИ	Теория диффузии инноваций
ТПК	Теория положений о криминологии
УЗ	уровень защищенности
Ц	целостность
ФЗ	Федеральный закон
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба технического и экспортного контроля Российской Федерации
CEH	*Certified Ethical Hacker*
CVE	*Common Vulnerabilities and Exposures*
IoT	*Internet of things*
IRC	*Internet-Relay-Chat*
OSI	*Open Systems Interconnection model*
PDCA	*Plan – Do – Check – Act*
TOR	*The Onion Router*
VPN	*Virtual Private Network*

Список литературы

1 Российская Федерация. Законы. О персональных данных : Федеральный закон № 152-ФЗ : [принят Государственной думой 8 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года] : (редакция от 24.04.2020). – Доступ из справ.-правовой системы Гарант. – Текст : электронный.

2 Российская Федерация. Законы. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : Приказ ФСТЭК России № 21 от 18 февраля 2013 г. – Доступ из справ.-правовой системы Гарант. – Текст : электронный.

3 Российская Федерация. Законы. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : Приказ ФСТЭК России № 17 от 11 февраля 2013 г. – Доступ из справ.-правовой системы Гарант. – Текст : электронный.

4 Российская Федерация. Законы. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации : Приказ ФСТЭК России № 239 от 25 декабря 2017 г. : (редакция от 26.03.2019). – Доступ из справ.-правовой системы Гарант. – Текст : электронный.

5 Методический документ : Методика оценки угроз безопасности информации : [утвержден ФСТЭК России 5 февраля 2021 г.]. – Доступ из справ.-правовой системы Гарант. – Текст : электронный.

6 Банк данных угроз БИ ФСТЭК России : [сайт]. – URL : https://bdu.fstec.ru/ (дата обращения: 17.11.2019). – Текст : электронный.

7 Список уязвимостей ФСТЭК России : [сайт]. – URL : https://bdu.fstec.ru/vul/ (дата обращения: 17.11.2019). – Текст : электронный.

8 Методический документ : Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации : [утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. N 149/54-144]. – Доступ из справ.-правовой системы Гарант. – Текст : электронный.

9 *BSI-Standard 100-1: Information Security Management Systems (ISMS)* = Система управления информационной безопасностью (СУИБ). – 2008. – версия 1.5. – 38 с. – *URL : https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStanda*

rds/standard_100-1_e_pdf.pdf?__blob=publicationFile (дата обращения: 08.07.2021). – Текст : электронный.

10 *BSI-Standard 100-2: IT-Grundschutz Methodology* = Методология «ИТ-Грундшутц». – 2005. – версия 1.0. – 74 с. – *URL : https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile* (дата обращения: 08.07.2021). – Текст : электронный.

11 *BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz* = Анализ рисков на базе «ИТ-Грундшутц». – 2005. – версия 2.0. – 19 с. – *URL : https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-3_e_pdf.pdf?__blob=publicationFile* (дата обращения: 08.07.2021). – Текст : электронный.

12 *IT-Grundschutz Catalogues* = Каталоги «ИТ-Грундшутц». – 2014. – версия 14.0. – 4618 с. – *URL : https://oiipdf.com/download/14198* (дата обращения: 08.07.2021). – Текст : электронный.

13 Международный стандарт *ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements // M.: ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection.* – 2013. – 25 с. – Текст : электронный (дата обращения: 08.07.2021).

14 Международный стандарт *BS 7799-2: 2002* Система управления информационной безопасностью – Инструкция по применению. *// M: BSI – DISC BDD/2 Information Security Management.* – 2002. – 55 с. – Текст : электронный (дата обращения: 08.07.2021).

15 Международный стандарт *National Institute of Standards and Technology Special Publication 800-30. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology // M: National Institute of Standards and Technology. Technology Administration U.S. Department of Commerce.* – 2002. – 54 с. – Текст : электронный (дата обращения: 08.07.2021).

16 Международный стандарт *BS ISO/IEC 27005:2008 Information technology – Security techniques – Information security risk management // M.: BSI – DISC BDD/2? Information Security Management.* – 2008. – 64 с. – Текст : электронный (дата обращения: 08.07.2021).

17 Международный стандарт *National Institute of Standards and Technology Special Publication 800-51 : Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme. Recommendations of the National Institute of Standards and Technology // National Institute of Standards and Technology.*

Technology Administration U.S. Department of Commerce. – 2002. – 5 с. – Текст : электронный (дата обращения: 08.07.2021).

18 Финогеев, А. А. Оценка информационных рисков в распределенных системах обработки данных на основе беспроводных сенсорных сетей / А. А. Финогеев, А. Г. Финогеев, И. С. Нефедова. – Текст : электронный // Электронная библиотека : КиберЛенинка : [сайт]. – 2016. – 12 с. – DOI : *https://doi.org/10.21685/2072-3059-2016-2-4*. – *URL : https://cyberleninka.ru/article/n/otsenka-informatsionnyh-riskov-v-raspredelennyh-sistemah-obrabotki-dannyh-na-osnove-besprovodnyh-sensornyh-setey/viewer* (дата обращения: 08.07.2021).

19 Белокурова, Е. В. Способы оценки угроз безопасности конфиденциальной информации для информационно-телекоммуникационных систем / Е. В. Белокурова, А. А. Дерканосова, А. А. Змеев [и др.]. – Текст : электронный // Электронная библиотека : КиберЛенинка : [сайт]. – 2015. – 6 с. – URL : https://cyberleninka.ru/article/n/sposoby-otsenki-ugroz-bezopasnosti-konfidentsialnoy-informatsii-dlya-informatsionno-telekommunikatsionnyh-sistem/viewer (дата обращения: 08.07.2021).

20 Коробейникова, А. Г. *Mathematical model for calculation of information risks for information and logistics system* = Математическая модель расчета информационных рисков для информационно-логистической системы / А. Г. Коробейникова, А. Ю. Гришенцев, И. Э. Комарова [и др.]. – Текст : электронный // Электронная библиотека : КиберЛенинка : [сайт]. – 2015. – 8 с. – URL : https://cyberleninka.ru/article/n/matematicheskaya-model-rascheta-informatsionnyh-riskov-dlya-informatsionno-logisticheskoy-sistemy/viewer (дата обращения: 08.07.2021).

21 Козин, И. С. Метод обеспечения безопасной обработки персональных данных на основе применения технологии блокчейн / И. С. Козин. – Текст : электронный // Электронная библиотека : КиберЛенинка : [сайт]. – 2019. – 9 с. – URL : *https://cyberleninka.ru/article/n/metod-obespecheniya-bezopasnoy-obrabotki-personalnyh-dannyh-na-osnove-primeneniya-tehnologii-blokcheyn/viewer* (дата обращения: 08.07.2021).

22 МакДональд Д. *Cyber/physical security vulnerability assessment integration* = Интеграция оценки уязвимости кибер / физической безопасности / Д. МакДональд, С. Клемент, С. Патрик [и др.] // *IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*. – 2013. – DOI : *https://doi.org/10.1109/ISGT.2013.6497883*. – Текст : электронный (дата обращения: 08.07.2021).

23 Хентеа М. *Improving Security for SCADA Control Systems* = Повышение безопасности систем управления SCADA/ М. Хентеа // *Interdisciplinary Journal of Information, Knowledge, and Management*. – 2008 - № 3. 14 с. [ЭЛЕКТРОННЫЙ РЕСУРС] // URL:

https://www.informingscience.org/Publications/3185?Source=%2FConferences%2FInSITE2008%2FProceedings (дата обращения: 08.07.2021).

24 Губарева, О. Ю. Оценка рисков информационной безопасности в телекоммуникационных сетях / О. Ю. Губарева. – Текст : электронный // Электронная библиотека : КиберЛенинка : [сайт]. – 2013. – 7 с. – *URL : https://cyberleninka.ru/article/n/otsenka-riskov-informatsionnoy-bezopasnosti-v-telekommunikatsionnyh-setyah/viewer* (дата обращения: 08.07.2021).

25 Рытов, М. Ю. Применение методологии stride для определения актуальных угроз безопасности программно-определяемых сетей / М. Ю. Рытов, Р. Ю. Калашников. – Текст : электронный // Электронная библиотека : КиберЛенинка : [сайт]. – 2019. – 6 с. – *URL : https://cyberleninka.ru/article/n/primenenie-metodologii-stride-dlya-opredeleniya-aktualnyh-ugroz-bezopasnosti-programmno-opredelyaemyh-setey/viewer* (дата обращения: 08.07.2021).

26 Абдо Х. А *safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis* = Подход к анализу рисков безопасности / защиты промышленных систем управления: кибер-бабочка - объединение новой версии дерева атак с анализом бабочки / Х. Абдо, Д. Флаус, Ф. Массе [и др.] // *Computers & Security*. – 2018. – № 72. – С. 175–195. – *DOI : https://doi.org/10.1016/j.cose.2017.09.004*. – Текст : электронный (дата обращения: 08.07.2021).

27 Касола В. *Toward the automation of threat modeling and risk assessment in IoT systems* = На пути к автоматизации моделирования угроз и оценки рисков в системах интернета вещей / В. Касола, А. Бенедиктис, М. Рак [и др.] // *Internet of Things*. – 2019. – № 7. – С. 1–13. – *DOI : https://doi.org/10.1016/j.iot.2019.100056*. – Текст : электронный (дата обращения: 08.07.2021).

28 Брачо А. А *simulation-based platform for assessing the impact of cyberthreats on smart manufacturing systems* = Платформа на основе моделирования для оценки воздействия киберугроз на интеллектуальные производственные системы / А. Брачо, К. Сэйгин, Х. Ван [и др.] // *Procedia Manufacturing*. – 2018. – № 26. – С. 1116–1127. – *DOI : https://doi.org/10.1016/j.promfg.2018.07.148*. – Текст : электронный (дата обращения: 08.07.2021).

29 Чжан В. *Armor PLC: A Platform for Cyber Security Threats Assessments for PLCs* = Броня PLC : Платформа для оценки угроз кибербезопасности для PLC / В. Чжан, И. Цзяо, Д. Ву [и др.] // *Procedia Manufacturing*. – 2020. – № 39. – С. 270–278. – *DOI : https://doi.org/10.1016/j.promfg.2020.01.334*. – Текст : электронный (дата обращения: 08.07.2021).

30 Черданцева Ю. А *Review of cyber security risk assessment methods for SCADA systems* = Обзор методов оценки рисков кибербезопасности для SCADA-систем / Ю. Черданцева, П. Бурнапа, А. Блит [и др.] // Computers & Security. – 2016. – № 56 (56). – *DOI :* https://doi.org/10.1016/j.cose.2015.09.009. – Текст : электронный (дата обращения: 08.07.2021).

31 Куре Х. И. *An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System* = Комплексный подход к управлению рисками кибербезопасности для киберфизической системы / Х. И. Куре, С. Ислам, М. А. Раззак // Applied Sciences. – 2018. – № 8 (6). – *DOI :* https://doi.org/10.3390/app8060898. – Текст : электронный (дата обращения: 08.07.2021).

32 Чои С. А *Study on Analysis of Malicious Code Behavior Information for Predicting Security Threats in New Environments* = Исследование по анализу информации о поведении вредоносного кода для прогнозирования угроз безопасности в новых средах / С. Чои, Т. Ли, Д. Квак // KSII Transactions on Internet and Information Systems. – 2019. – № 13 (3). – С. 1611–1625. – *DOI :* https://doi.org/10.3837/tiis.2019.03.028. – Текст : электронный (дата обращения: 08.07.2021).

33 Фенг Б. *Stopping the Cyberattack in the Early Stage: Assessing the Security Risks of Social Network Users* = Остановка кибератаки на ранней стадии : Оценка рисков безопасности пользователей социальных сетей / Б. Фенг, Ц. Ли, Ю. Цзи [и др.] // *Hindawi magazine*. – 2019. – *DOI :* https://doi.org/10.1155/2019/3053418. – Текст : электронный (дата обращения: 08.07.2021).

34 Налини М. *Digital risk management for data attacks against state evaluation* = Цифровое управление рисками для атак на данные против оценки состояния / М. Налини, А. Чакрам // *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*. – 2020. – № 88. – *DOI :* https://doi.org/10.35940/ijitee.I1130.0789S419. – Текст : электронный (дата обращения: 08.07.2021).

35 Деб А. *Predicting Cyber Events by Leveraging Hacker Sentiment* = Прогнозирование кибер-событий с помощью настроений хакеров / А. Деб, К. Лерман, Э. Феррара // *Information*. – 2018. – № 9 (11). – С. 18. – *DOI :* https://doi.org/10.3390/info9110280. – Текст : электронный (дата обращения: 08.07.2021).

36 Ясасин Э. *Forecasting IT Security Vulnerabilities - An Empirical Analysis* = Прогнозирование уязвимостей ИТ-безопасности - эмпирический анализ / Э. Ясасин, Д. Престер, Г. Вагнер [и др.] // *Computers & Security*. – 2020. – № 88. – С. 1–24. – *DOI :* https://doi.org/10.1016/j.cose.2019.101610. – Текст : электронный (дата обращения: 08.07.2021).

37 Сюн Ц. *Construction of information network vulnerability threat assessment model for CPS risk assessment* = Построение модели оценки угроз уязвимости информационной сети для оценки рисков CPS / Ц. Сюн, Ц. Ву // *Computer Communications. – 2020. – № 155. – С. 197–204. – DOI : https://doi.org/10.1016/j.comcom.2020.03.026*. – Текст : электронный (дата обращения: 08.07.2021).

38 Похрел Н. Р. *Cybersecurity: Time Series Predictive Modeling of Vulnerabilities of Desktop Operating System Using Linear and Non-Linear Approach* = Кибербезопасность : Прогнозное моделирование временных рядов уязвимостей настольной операционной системы с использованием линейного и нелинейного подхода / Н. Р. Похрел, Х. Родриго, К. Цокос // *Journal of Information Security*. – 2017. – № 08 (04). – С. 362–382. – *DOI : https://doi.org/10.4236/jis.2017.84023*. – Текст : электронный (дата обращения: 08.07.2021).

39 Румани Д. *Time series modeling of vulnerabilities* = Моделирование временных рядов уязвимостей / Д. Румани, Д. Нванкпа, Я. Румани // *Computers & Security*. – 2015. – № 51. – С. 32–49. – *DOI : https://doi.org/10.1016/j.cose.2015.03.003*. – Текст : электронный (дата обращения: 08.07.2021)..

40 Феба Б. А *Review on Cybersecurity Threats and Statistical Models = Обзор угроз кибербезопасности и статистических моделей / Б. Феба, С. Кишор // IOP Conf. Series: Materials and Science Engineering. – 2018. – № 369. – DOI : https://doi.org/10.1088/1757-899X/396/1/012029*. – Текст : электронный (дата обращения: 08.07.2021).

41 Мовахеди Й. *Some Guidelines for Risk Assessment of Vulnerability Discovery Processes* = Некоторые рекомендации по оценке рисков процессов обнаружения уязвимостей / Й. Мовахеди // *University of Maryland*. – 2019. – *DOI : https://doi.org/10.13016/ypw6-k7ge*. – Текст : электронный (дата обращения: 08.07.2021)..

42 Мовахеди Й. *Cluster-based vulnerability assessment of operating systems and web browsers* = Кластерная оценка уязвимости операционных систем и веб-браузеров / Й. Мовахеди, М. Кукье, И. Гаши [и др.] // *Computing*. – 2019. – № 101 (2). – *DOI : https://doi.org/10.1007/s00607-018-0663-0*. – Текст : электронный (дата обращения: 08.07.2021)..

43 Мовахеди Й. *Vulnerability prediction capability: A comparison between vulnerability discovery models and neural network models* = Возможность прогнозирования уязвимостей : Сравнение моделей обнаружения уязвимостей и моделей нейронных сетей/ Й. Мовахеди, М. Кукье, И. Гаши // *Computers & Security*. – 2019. – № 87. – *DOI : https://doi.org/10.1016/j.cose.2019.101596*. – Текст : электронный (дата обращения: 08.07.2021).

44 Стакмэн Д. *The Effect of Dimensionality Reduction on Software Vulnerability Prediction Models* = Влияние уменьшения размерности на модели прогнозирования уязвимости программного обеспечения / Д. Стакмэн, Д. Волден, Р. Скандариато // *IEEE Transactions on Reliability*. – 2017. – № 66 (1). – С. 17–37. – *DOI : http://dx.doi.org/10.1109/TR.2016.2630503*. – Текст : электронный (дата обращения: 08.07.2021).

45 Хаускен К. *The dynamics of crime and punishment* = Динамика преступности и наказания / К. Хаусен, Д. Ф. Мокснес // *International Journal of Modern Physics*. – 2005. – № 16 (11). – С. 1701–1732. – *DOI : http://dx.doi.org/10.1142/S0129183105008229*. – Текст : электронный (дата обращения: 08.07.2021).

46 Бэкер Г. С. Экономика преступности = Экономика преступности / Г. С. Бэкер // *Cross Sections, Federal Reserve Bank of Richmond*. – 1995. – № 12. – С. 8–15. – *DOI : https://doi.org/10.1016/S0313-5926(87)50021-2*. – Текст : электронный (дата обращения: 27.04.2020).

47 Бернулли Д. Опыт новой теории измерения жребия : Теория потребительского поведения и спроса / Д. Бернулли // Вехи экономической мысли. – Т.1. – Под ред. В.М.Гальперина. – СПб. : Экономическая школа. – 1999. – С. 11-27. – Текст : электронный.

48 Рогерс Э. *Diffusion of Innovations* = Распространение инноваций / Э. Рогерс, А. Сингал, М. М. Квинлан // *New York: Free Press*. – 2002. – *DOI : https://doi.org/10.4324/9780203710753-35*. – Текст : электронный (дата обращения: 08.07.2021).

49 Бас Ф. *A new product growth model for consumer durables* = Новая модель роста потребительских товаров длительного пользования / Ф. Бас // *INFORMS*. – 1969. – № 15 (5). – С. 215–227. – *DOI : https://doi.org/10.1287/mnsc.15.5.215*. – Текст : электронный (дата обращения: 08.07.2021).

50 Мансфилд Э. *Technical Change and the Rate of Imitation* = Технические изменения и скорость имитации / Э. Мансфилд // *The Econometric Society*. – 1961. – № 29 (4). – *DOI : https://doi.org/10.2307/1911817*. – *Текст : электронный (дата обращения: 08.07.2021)*

51 Хагерстранд Т. *Innovation diffusion as a spatial process*= Дифуззия инновации как пространственный процесс / Т. Хагерстранд // *Chicago, University of Chicago Press. – 1967. – DOI : https://doi.org/10.1111/j.1538-4632.1969.tb00626.x*. – Текст : электронный (дата обращения: 08.07.2021).

52 О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон № 187-ФЗ: [принят Государственной думой

12 июля 2017 года]. – Доступ из справ.-правовой системы Гарант. – Текст: электронный.

53 Российская Федерация. Законы. Об утверждении требований к защите персональных данных при их обработке в ИС персональных данных : Постановление Правительства РФ № 1119 : [утверждено 1 ноября 2012 г.]. – Доступ из справ.-правовой системы Гарант. – Текст : электронный.

54 Российская Федерация. Законы. Об утверждении правил категорирования объектов критической информационной инфраструктуры РФ, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений : Постановление Правительства РФ № 127 : [утверждено 8 февраля 2018 г.] : (редакция от 13.04.2019). – Доступ из справ.-правовой системы Гарант. – Текст : электронный.

55 Российская Федерация. Законы. Об утверждении Единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел "Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации" : Приказ Минздравсоцразвития РФ № 205 : [утвержден 22 апреля 2009 г.]. – Доступ из справ.-правовой системы Гарант. – Текст : электронный.

56 Гаськова Д. А. Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры / Д. А. Гаськова, А. Г. Массель. – Текст : электронный // Электронная библиотека : КиберЛенинка : [сайт]. – 2019. – 9 с. – *DOI: https://doi.org/10.21681/2311-3456-2019-2-42-49*. – *URL : https://cyberleninka.ru/article/n/tehnologiya-analiza-kiberugroz-i-otsenka-riskov-narusheniya-kiberbezopasnosti-kriticheskoy-infrastruktury/viewer* (дата обращения: 08.07.2021).

57 Попова Е. В. Метод выбора системы защиты информации с учетом критерия конкурентоспособности предприятия / Е. В. Попопа. – Текст : электронный // Электронная библиотека : КиберЛенинка : [сайт]. – 2016. – 6 с. – *DOI: https://doi.org/10.15217/issn1684-8853.2016.6.85*. – *URL : https://cyberleninka.ru/article/n/metod-vybora-sistemy-zaschity-informatsii-s-uchetom-kriteriya-konkurentosposobnosti-predpriyatiya/viewer* (дата обращения: 08.07.2021).

58 Клюев А. С. Оценка рисков в функционирующей информационной системе / А. С. Клюев, А. А. Файзенгер, Д.Р. Юрьев // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2018. – № 5. – С. 105-109. – Текст : электронный.

59 Чжан Т. *Research on Privacy Security Risk Assessment Method of Mobile Commerce Based on Information Entropy and Markov = Исследование метода оценки рисков безопасности конфиденциальности в мобильной коммерции на основе информационной энтропии и Маркова / Т. Чжан, К. Чжао, М. Янг [и др.] // Hindawi magazine.* – 2020. – *DOI :* https://doi.org/10.1155/2020/8888296. – Текст : электронный (дата обращения: 08.07.2021).

60 Виджаянто Р. М. *Enhancing is Risk Assessment through using Combination Vector Matrix and Octave Methods* = Повышение качества оценки рисков за счет использования комбинированных векторных матричных и октавных методов / Р. М. Виджаянто // *International Journal of Advanced Trends in Computer Science and Engineering.* – 2019. – № 8 (6). – *DOI :* https://doi.org/10.30534/ijatcse/2019/77862019. – Текст : электронный (дата обращения: 08.07.2021).

61 Меланд П. Х. *An Experimental Evaluation of Bow-Tie Analysis for Cybersecurity Requirements: Methods and Protocols* = Экспериментальная оценка анализа "Бабочка" для требований кибербезопасности : Методы и протоколы / П. Х. Меланд, К. Бернсмен, К. Фрестайд [и др.] // *Information & Computer Security.* – 2019. – № 27 (4). – *DOI :* https://doi.org/10.1007/978-3-030-12786-2_11. – Текст : электронный (дата обращения: 08.07.2021).

62 Бабенко А. А. Модель профиля угроз информационной безопасности корпоративной информационной системы / А. А. Бабенко, С. С. Козунова. – Текст : электронный // Электронная библиотека : КиберЛенинка : [сайт]. – 2018. – 6 с. – *URL :* https://cyberleninka.ru/article/n/model-profilya-ugroz-informatsionnoy-bezopasnosti-korporativnoy-informatsionnoy-sistemy/viewer (дата обращения: 08.07.2021).

63 Зикратов И. А. *Evaluation of information security in cloud computing based on the bayesian approach* = Оценка информационной безопасности в облачных вычислениях на основе байесовского подхода / И. А. Зикратов, С. В. Одегов. – Текст : электронный // Электронная библиотека : КиберЛенинка : [сайт]. – 2012. – 6 с. – *URL :* https://cyberleninka.ru/article/n/otsenka-informatsionnoy-bezopasnosti-v-oblachnyh-vychisleniyah-na-osnove-bayesovskogo-podhoda/viewer (дата обращения: 08.07.2021).

64 Дерендяев Д. А. Алгоритм оценки значения остаточных рисков угроз информационной безопасности с учетом разделения механизмов защиты на типы / Д. А. Дерендяев, Ю. А. Гатчин, В. А. Безруков. – Текст : электронный // Электронная библиотека : КиберЛенинка : [сайт]. – 2018. – 4 с. – *URL :* https://cyberleninka.ru/article/n/algoritm-otsenki-znacheniya-ostatochnyh-riskov-ugroz-informatsionnoy-bezopasnosti-s-uchetom-razdeleniya-mehanizmov-zaschity-na-tipy/viewer (дата обращения: 08.07.2021).

65 Кадочникова Н. А. Оценка рисков информационной безопасности на основе метода построения матрицы *GENERAL ELECTRIC/MCKINSEY* / Н. А. Кадочникова, В. Ф. Цырульник. – Текст : электронный // Электронная библиотека : Elibrary : [сайт]. – 2015. – *DOI : https://doi.org/10.17117/na.2015.11.03.156*. – *URL : https://cyberleninka.ru/article/n/razrabotka-sistemy-podderzhki-prinyatiya-resheniya-dlya-otsenki-riskov-i-ugroz-natsionalnoy-bezopasnosti/viewer* (дата обращения: 08.07.2021).

66 Скворцова М. А. Разработка системы поддержки принятия решения для оценки рисков и угроз национальной безопасности / М. А. Скворцова, В. И. Терехов. – Текст : электронный // Электронная библиотека : КиберЛенинка : [сайт]. – 2018. – 11 с. – *URL : https://cyberleninka.ru/article/n/razrabotka-sistemy-podderzhki-prinyatiya-resheniya-dlya-otsenki-riskov-i-ugroz-natsionalnoy-bezopasnosti/viewer* (дата обращения: 08.07.2021).

67 Кузнецов Н. А. Модель автоматизированной системы оптимизации параметров управления рисками в терминах угроз, уязвимостей и резервов / Н. А. Кузнецов, А. А. Мозоль. – Текст : электронный // Электронная библиотека : КиберЛенинка : [сайт]. – 2019. – 7 с. – *URL : https://cyberleninka.ru/article/n/model-avtomatizirovannoy-sistemy-optimizatsii-parametrov-upravleniya-riskami-v-terminah-ugroz-uyazvimostey-i-rezervov/viewer* (дата обращения: 08.07.2021).

68 Плетнев П. В. Методика количественного определения рисков ИБ / П. В. Плетнев, В. М. Белов. – Текст : электронный // Электронная библиотека : КиберЛенинка : [сайт]. – 2011. – 5 с. – *URL : https://cyberleninka.ru/article/n/metodika-kolichestvennogo-opredeleniya-riskov-ib/viewer* (дата обращения: 08.07.2021).

69 Ализера С. *Realtime intrusion risk assessment model based on attack and service dependency graphs* = Модель оценки риска вторжения в реальном времени на основе графиков зависимостей от атак и услуг / С. Ализера, М. Дагенаис, Л. Ванг // *Computer Communications*. – 2017. – № 116. – С. 253–272. – *DOI : https://doi.org/10.1016/j.comcom.2017.12.003*. – Текст : электронный (дата обращения: 08.07.2021).

70 Шмитц К. *Lightweight Security Risk Assessment for decision support in information security* = Упрощенная оценка рисков безопасности для поддержки принятия решений в области информационной безопасности / К. Шмитц, С. Пейп // *Computers & Security*. – 2020. – № 90. – С. 1–20. – *DOI : https://doi.org/10.1016/j.cose.2019.101656*. – Текст : электронный (дата обращения: 08.07.2021)..

71 Хашим Н. А. *Risk Assessment Method for Insider Threats in Cyber Security: A review* = Метод оценки рисков инсайдерских угроз в кибербезопасности : Обзор / Н. А. Хашим, З. Зайнал, П. А. Перумал [и др.] // *International Journal*

of Advanced Computer Science and Applications. – 2018. – № 9 (11). – *DOI :* https://doi.org/10.14569/IJACSA.2018.091119. – Текст : электронный (дата обращения: 08.07.2021).

72 Ху З. *Analytical Assessment of Security Level of Distributed and Scalable Computer Systems* = Аналитическая оценка уровня безопасности распределенных и масштабируемых компьютерных систем/ З. Ху, В. Мухин, Я. Корнага [и др.] // *International Journal of Intelligent Systems and Applications.* – 2016. – № 12. – *DOI :* https://doi.org/10.5815/ijisa.2016.12.07. – Текст : электронный (дата обращения: 08.07.2021).

73 Ванг З. *Risk Automatic cyber security risk assessment based on fuzzy fractional ordinary differential equations* = Автоматическая оценка рисков кибербезопасности на основе нечетких дробных обыкновенных дифференциальных уравнений / З. Ванг, Л. Чен, С. Сонг [и др.] // *Alexandria Engineering Journal.* – 2020. – № 59 (4). – *DOI :* https://doi.org/10.1016/j.aej.2020.05.014. – Текст : электронный (дата обращения: 08.07.2021).

74 Зарех, А. *Risk Assessment for Cyber Security of Manufacturing Systems: A Game Theory Approach* = Оценка рисков для кибербезопасности производственных систем : Подход теории игр / А. Зарех, Х. Ван, Й. Ли [и др.] // *Procedia Manufacturing.* – 2019. – № 38. – *DOI :* https://doi.org/10.31224/osf.io/mb5t9. – Текст : электронный (дата обращения: 08.07.2021).

75 Санчо Д. *New approach for threat classification and security risk estimations based on security event management* = Новый подход к классификации угроз и оценке рисков безопасности на основе управления событиями безопасности / Д. Санчо, А. Каро // *FutureGenerationComputerSystems.* – 2020. – № 113. – С. 488–505. – *DOI :* https://doi.org/10.1016/j.future.2020.07.015. – Текст : электронный (дата обращения: 08.07.2021).

76 Шольц Р. В. *Organizational vulnerability of digital threats: A first validation of an assessment method* = Организационная уязвимость цифровых угроз: первая проверка метода оценки / Р. В. Шольц // *European Journal of Operational Research. – 2020. – № 282. – С. 627–643. – DOI :* https://doi.org/10.1016/j.ejor.2019.09.020. *– Текст : электронный (дата обращения: 08.07.2021).*

77 *Зуев, П. Methods of cyber security assessment in the information and telecommunications system* = Методы оценки кибербезопасности в информационно-телекоммуникационной системе / П. Зуев, О. Сальникова, О. Мазулевский [и др.] // *International Journal of Advanced Trends in Computer Science and Engineering.* – 2020. – № 9 (5). – С. 6990–6994. – *DOI :*

https://doi.org/10.30534/ijatcse/2020/17952020. – Текст : электронный (дата обращения: 08.07.2021).

78 Ганин А. А. *Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management* = Многокритериальная система принятия решений для оценки и управления рисками кибербезопасности / А. А. Ганин, П. Квач, М. Панвар [и др.] // *Risk Analysis Volume.* – 2020. – № 40 (1). – С. 183–199. – *DOI : https://doi.org/10.1111/risa.12891*. – Текст : электронный (дата обращения: 08.07.2021).

79 Фигейра П. *Improving information security risk analysis by including threat-occurrence predictive models* = Улучшение анализа рисков информационной безопасности за счет включения моделей прогнозирования возникновения угроз / П. Фигейра, К. Браво-Лопез, Д. Л. Лопез-Ривас // *Computers and Security Volume. – 2020.* – № 88 (101609). – *DOI : https://doi.org/10.1016/j.cose.2019.101609*. – Текст : электронный (дата обращения: 08.07.2021).

80 Ермалович П. *Formalization of Attack Prediction Problem* = Формализация задачи прогнозирования атаки / П. Ермолович, М. Меджри. – Текст : электронный // *IEEE Explore Digital Library*. – 2018. – С. 280–286. – *URL : https://www.academia.edu/43299572/Formalization_of_attack_prediction_problem* – Текст : электронный (дата обращения: 08.07.2021).

81 *Сантини П. A Data-Driven Approach to Cyber Risk Assessment* = Подход к оценке киберрисков на основе данных / П. Сантини, Д. Готтарди, М. Бальди, Ф. Кьяралюс // *Security and Communication Networks Volume.* – 2019. – 8 с. – *DOI : https://doi.org/10.1155/2019/6716918*. – Текст : электронный (дата обращения: 08.07.2021).

82 Кетабдар Х. *Network security risk analysis using attacker's behavioral parameters* = Анализ рисков сетевой безопасности с использованием поведенческих параметров злоумышленника / Х. Кетабдар, Р. Резаее, А. Гэмибафхи, М. Хосрави-Фармад // *International Conference on Computer and Knowledge Engineering (ICCKE).* – 2016. – *DOI : https://doi.org/10.1109/ICCKE.2016.7802161*. – Текст : электронный (дата обращения: 08.07.2021).

83 Гусак М. *Survey of Attack Projection, Prediction, and Forecasting in Cyber Security* = Обзор прогнозирования атак в области кибербезопасности / М. Гусак, Э. Бу-Харб, П. Селеда // *IEEE Communications Surveys & Tutorials*. – 2018. – С. 99. – *DOI : https://doi.org/10.1109/COMST.2018.2871866*. – Текст : электронный (дата обращения: 08.07.2021).

84 Сингх А. *Database intrusion detection using role and user behavior based risk assessment* = Обнаружение вторжений в базу данных с использованием оценки рисков на основе ролей и поведения пользователей / А. Сингх, Н.

Кумар, Т. Шарма // *Journal of Information Security and Applications*. – 2020. – № 55 (102654). – *DOI :* https://doi.org/10.1016/j.jisa.2020.102654. – Текст : электронный (дата обращения: 08.07.2021).

85 Хоумер М. *A risk and security assessment of VANET availability using attack tree concept* = Оценка рисков и безопасности доступности VANET с использованием концепции дерева атак / М. Хоумер, М. Л. Хаснауи // *International Journal of Electrical and Computer Engineering*. – 2020. – № 10 (6). – С. 6039–6044. – *DOI :* http:/./doi.org/10.11591/ijece.v10i6.pp6039-6044. – Текст : электронный (дата обращения: 08.07.2021).

86 Максименко В. Н. Основные подходы к анализу и оценке рисков информационной безопасности / В. Н. Максименко, Е. В. Ясюк. – Текст : электронный // Электронная библиотека : КиберЛенинка : [сайт]. – 2017. – 7 с. – *URL :* https://cyberleninka.ru/article/n/osnovnye-podhody-k-analizu-i-otsenke-riskov-informatsionnoy-bezopasnosti/viewer (дата обращения: 08.07.2021).

87 Куркина, Е. П. Оценка риска: экспертный метод / Е. П. Куркина, Д. Г. Шувалова. – Текст : электронный // Электронная библиотека : КиберЛенинка : [сайт]. – 2017. – 7 с. – *URL :* https://cyberleninka.ru/article/n/otsenka-riska-ekspertnyy-metod/viewer (дата обращения: 08.07.2021).

88 Фролов, А. А. Исследование механизмов распространения запрещенного содержимого в *DarkNet* / А. А. Фролов., Д. С. Сильнов. – Текст : электронный // Электронная библиотека : КиберЛенинка : [сайт]. – 2017. – 9 с. – *DOI* : 10.25559. – *URL :* https://cyberleninka.ru/article/n/issledovanie-mehanizmov-rasprostraneniya-zapreschennogo-soderzhimogo-v-darknet/viewer (дата обращения: 08.07.2021).

89 Паспорт федерального проекта «Информационная безопасность» : Утвержден Правительственной комиссией по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности : [протокол от 28 мая 2019 г. №6]. – Текст : электронный.

90 *The Global Risks Report* 2018 = Отчет о глобальных рисках за 2018 год // *MARSH&McLENNAN COMPANIES*. – 2018. – № 13. – С. 80. – *URL :* https://www.marsh.com/us/insights/research/the-global-risks-report-2018.html (дата обращения: 27.04.2020)– Текст : электронный.

91 Кибербитва на *PHDays*, или Как за 30 часов взломать городскую инфраструктуру. – Текст. Изображение : электронные // *Positive Hack Days :* [сайт]. – 2018. – *URL :* https://www.phdays.com/ru/press/news/kiberbitva-na-phdays-ili-kak-za-30-chasov-vzlomat-gorodskuyu-infrastrukturu/ (дата обращения: 27.04.2020).

92 *PHDays:* точно в девятку. – Текст. Изображение : электронные // *Positive Hack Days* : [сайт]. – 2019. – *URL :* https://www.phdays.com/ru/press/news/phdays-tochno-v-devyatku/ (дата обращения: 27.04.2020).

93 В РЖД заявили о небольшом ущербе от атаки вируса *WannaCry*. – Текст : электронный // Интерфакс : [сайт]. – 2017. – *URL :* https://www.sport-interfax.ru/wc2018/563900 (дата обращения: 17.11.2019).

94 Трунина, А. «Роснефть» сообщила о мощной хакерской атаке на свои серверы / А. Трунина., И. Рождественский, А. Фадеева, А. Вовнякова. – Текст : электронный // РБК : [сайт]. – 2017. – 27 июня. – *URL :* https://www.rbc.ru/technology_and_media/27/06/2017/595247629a7947dc9d430d2c/ (дата обращения: 17.11.2019).

95 Чернышова, Е. Сбербанк назвал версии утечки данных своих клиентов / Е. Чернышова., А. Фейнберг. – Текст : электронный // РБК : [сайт]. – 2019. – 3 октября. – *URL :* https://www.rbc.ru/finances/03/10/2019/5d960ab29a79471ea76e1769 (дата обращения: 17.11.2019).

96 ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения = *Protection of information. Object of informatisation. Factors influencing the information. General* : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374-ст : введен впервые : дата введения 2008-01-02 / разработан ФГУ ГНИИИ ПТЗИ ФСТЭК России. – Москва : Стандартинформ, 2007. – Доступ из справ.-правовой системы Гарант. – Текст : электронный.

97 Коди Т. *A utilitarian approach to adversarial learning in credit card fraud detection* = Утилитарный подход к состязательному обучению в выявлении мошенничества с кредитными картами / Т. Коди, С. Адамс, П. Белинг // *Institute of Electrical and Electronics Engineers Inc. Conference paper «Systems and Information Engineering Design Symposium»*. – 2018. – С. 237–242. – *DOI :* http://dx.doi.org/10.1109/SIEDS.2018.8374743. – Текст : электронный (дата обращения: 08.07.2021).

98 Паскье Р. *Measurement system design for civil infrastructure using expected utility* = Проектирование системы измерения для гражданской инфраструктуры с использованием ожидаемой полезности / Р. Паскье, Д. Гуле, А. Смит // *Elsevier Ltd. Advanced Engineering Informatics. – 2017. – № 32. – С. 40–51. – DOI :* https://doi.org/10.1016/j.aei.2016.12.002. – Текст : электронный (дата обращения: 08.07.2021).

99 Данилов Н. Н. Курс математической экономики / Н. Н. Данилов. – Санкт-Петербург : Издательство "Лань". – 2016. – 400 с. – Библиогр.: с. 116–118. — ISBN 978-5-8114-2172-5. – Текст : электронный.

100 Эрлих И. *Participation in illegitimate activities: theoretical and empirical investigation* = Участие в незаконной деятельности / И. Эрлих // *J. of Publ. Econ.* – 1973. – № 81 (3). – С. 521–565. – *DOI : http://dx.doi.org/10.1086/260058*. – Текст : электронный (дата обращения: 08.07.2021).

101 Ганичева А. В. Математические модели и методы оценки событий, ситуаций и процессов / А. В. Ганичева. – Санкт-Петербург : Издательство "Лань". – 2017. – 188 с. – Библиогр.: с. 107–110. — ISBN 978-5-8114-2419-1. – Текст : электронный.

102 Долан М. *Violence risk prediction: Clinical and actuarial measures and the role of the Psychopathy Checklist* = Прогнозирование риска насилия: клинические и актуарные меры и роль контрольного списка по психопатии / М. Долан // *The British Journal of Psychiatry.* – 2000. – № 177 (4). – С. 303–311. – *DOI : http://dx.doi.org/10.1192/bjp.177.4.303*. – Текст : электронный (дата обращения: 08.07.2021).

103 Генпрокуратура составила портрет типичного российского хакера. – Текст : электронный // Ведомости : [сайт]. – 2018. – *URL : https://www.vedomosti.ru/technology/news/2018/12/11/788967-sostavila* (дата обращения: 27.04.2020).

104 Киберпреступность и киберконфликты. – Текст : электронный // TADVISER: [сайт]. – 2021. – *URL : https://www.tadviser.ru/index.php/Статья:Киберпреступность_и_киберконфликты_:_Россия* (дата обращения: 27.04.2020).

105 Потери банков от киберпреступности. – Текст : электронный // *TADVISER: [сайт]*. – 2021. – *URL : https://www.tadviser.ru/index.php/_Статья:_Потери_банков_от_киберпреступности* (дата обращения: 27.04.2020).

106 Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности Банка России 01.09.2017 – 31.08.2018. – Текст. Изображение : электронные // Банк России : [сайт]. – 2018. – *URL : http://www.cbr.ru/Collection/Collection/File/32088/survey_0917_0818.pdf* (дата обращения: 27.04.2020).

107 Обзор основных типов компьютерных атак в кредитно-финансовой сфере в 2018 году. – Текст. Изображение : электронные // Банк России : [сайт]. – 2018. – *URL :*

http://www.cbr.ru/collection/collection/file/32085/dib_2018_20190704.pdf (дата обращения: 27.04.2020).

108 Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности Банка России 01.09.2018 – 31.08.2019. – Текст. Изображение : электронные // Банк России : [сайт]. – 2019. – *URL :* http://www.cbr.ru/Collection/Collection/File/32087/FINCERT_report_20191010.PDF (дата обращения: 17.11.2019).

109 *Petya*. А заработал на атаке всего $12,6 тыс. – Текст : электронный // News24UA *: [сайт*]. – 2017. – *URL :* https://news24ua.com/petya-zarabotal-na-atake-vsego-126-tys (дата обращения: 08.07.2021).

110 Проверка на прочность: зачем создатели вируса *BadRabbit* атаковали СМИ и банки. – Текст : электронный // *Forbes* : [сайт]. – 2017. – *URL :* https://www.forbes.ru/tehnologii/351955-proverka-na-prochnost-zachem-sozdateli-virusa-badrabbit-atakovali-smi-i-banki (дата обращения: 08.07.2021).

111 ЦБ раскрыл объем мошеннических списаний со счетов россиян в 2014 году. – Текст : электронный // РБК : [сайт]. – 2015. – *URL :* https://www.rbc.ru/finances/23/06/2015/558936aa9a79477bdc5736ec (дата обращения: 08.07.2021).

112 Мошенники в прошлом году украли у клиентов банков 6,4 млрд рублей. – Текст : электронный // Ведомости : [сайт]. – 2020. – *URL :* https://www.vedomosti.ru/personal_finance/articles/2020/02/19/823409-moshenniki-ukrali-64-mlrd-rub (дата обращения: 08.07.2021).

113 Основные типы компьютерных атак в кредитно-финансовой сфере в 2019–2020 годах. – Текст. Изображение : электронные // Банк России : [сайт]. – 2021. – *URL :* http://www.cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf (дата обращения: 08.07.2021).

114 4 млрд рублей украли мошенники со счетов клиентов банков в первом полугодии. – Текст : электронный // Ведомости : [сайт]. – 2017. – *URL :* https://www.vedomosti.ru/economics/articles/2020/11/01/845396-4-mlrd (дата обращения: 08.07.2021).

115 Зарплатный индекс *Superjob* сферы «Информационные технологии». – Текст. Изображение : электронные // *SuperJob* : [сайт]. – 2017. – *URL :* https://www.superjob.ru/paymentindex/it/#/31 (дата обращения: 08.07.2021).

116 Российская Федерация. Законы. Уголовный кодекс Российской Федерации : УК : [принят Государственной думой 24 мая 1996 года : одобрен Советом Федерации 5 июня 1996 года] : (редакция от 05.04.2021). – Доступ из справ.-правовой системы Гарант. – Текст : электронный.

117 *Petya (NotPetya) Attack* = Атака *Petya (NotPetya)*. – Текст : электронный // *ProofPoint* : [сайт]. – 2018. – *URL : https://www.proofpoint.com/us/threat-reference/petya* (дата обращения: 08.07.2021).

118 Спецслужбы ФРГ : вирус *Petya* позволяет красть данные. – Текст : электронный // ТАСС : [сайт]. – 2017. – *URL : https://tass.ru/mezhdunarodnaya-panorama/4396011* (дата обращения: 29.12.2020).

119 Новая эпидемия шифровальщика *Petya / NotPetya / ExPetr*. – Текст : электронный // Касперский : [сайт]. – 2017. – *URL : https://www.kaspersky.ru/blog/new-ransomware-epidemics/17855/* (дата обращения: 08.07.2021).

120 Анализ шифровальщика *Petya:* как развивалась атака. – Текст : электронный // *Emsisoft* : [сайт]. – 2017. – *URL : https://blog.emsisoft.com/ru/28057/%d0%b0%d0%bd%d0%b0%d0%bb%d0%b8%d0%b7-%d1%88%d0%b8%d1%84%d1%80%d0%be%d0%b2%d0%b0%d0%bb%d1%8c%d1%89%d0%b8%d0%ba%d0%b0-petya/* (дата обращения: 08.07.2021).

121 Величина МРОТ в 2013 – 2021 годах в России. – Текст : электронный // НАЛОГ-НАЛОГ.ру : [сайт]. – 2021. – *URL : https://nalog-nalog.ru/posobiya/posobie_po_vremennoj_netrudosposobnosti_bolnichnyj/velichina-mrot-v-rossii-tablica/* (дата обращения: 08.07.2021).

122 Зенебе А. *Cyber Threat Discovery from Dark Web* = Обнаружение киберугроз из Даркнета / А. Зенебе, М. Шумба, А. Карилло, С. Куэнка // *EPiC SeriesinComputing*. – 2019. – № 64. – С. 174–183. – *DOI : https://doi.org/10.1109/ICBDAA.2018.8629658*. – Текст : электронный (дата обращения: 08.07.2021).

123 Карта распространения сетевого червя *WannaCry*. – Изображение (картографическое; неподвижное; двухмерное) : электронное // *Intel :* [сайт]. – *URL : http://web.archive.org/web/20170519161205/https://intel.malwaretech.com/botnet/wcrypt/?t=24h&bid=all* (дата обращения: 08.07.2021).

124 *Q4 2020 Threat Report: A Quarterly Analysis of Cybersecurity Trends, Tactics and Themes* = Отчет об угрозах за 4 квартал 2020 года: Ежеквартальный анализ тенденций, тактики и тем в области кибербезопасности. – Текст. Изображение : электронные // *ProofPoint :* [сайт]. – *URL : https://www.proofpoint.com/us/blog/threat-insight/q4-2020-threat-report-quarterly-analysis-cybersecurity-trends-tactics-and-themes* (дата обращения: 08.07.2021).

125 Программный комплекс «Ampire» : Свидетельство о государственной регистрации программы для ЭВМ №2019613098, выданное Правообладателю – закрытому акционерному обществу «Перспективный мониторинг» (ЗАО «ПМ») 07.03.2019 г : [зарегистрирован в Едином реестре российских программ для электронных вычислительных машин и баз данных 20 сентября 2019 г.]. – Текст : электронный.

126 *A Cyber-Kill-Chain based taxonomy of crypto-ransomware features* = Таксономия функций крипто-вымогателей на основе Cyber-Kill-Chain / Т. Даргахи, А. Дехгантанья, М. Конти [и др.] // *Journal of Computer Virology and Hacking Techniques*. – 2019. – С. 277–305. – Ежекв. – Текст: электронный (дата обращения 08.12.2020).

127 *The Cyber Kill Chain framework* = Фреймворк The Cyber Kill Chain. – Текст: электронный. – Обновляется в течение суток. // *Lockheed Martin Corporation* : [официальный сайт]. – *URL : https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html* (дата обращения: 29.12.2020).

128 Скарфоне К. *Technical guide to information security testing and assessment* = Техническое руководство по тестированию и оценке информационной безопасности / К. Скарфоне, М. Суппайя, А. Коди, А. Оребо // *NIST Special Publication* 800-115. – 2008. – 80 с.

129 *MITRE ATT&CK Matrix for Enterprise* = Матрица MITRE ATT&CK для предприятия. – Текст: электронный // *MITRE ATT&CK* : [сайт]. – *URL : https://attack.mitre.org/matrices/enterprise/* (дата обращения: 29.12.2020).

130 *Certified Ethical Hacker CEH v11* = Сертифицированный этический хакер CEH v11 . – Текст. Изображение : электронные // *EC-Council :* [сайт]. – *URL : https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/* (дата обращения: 29.12.2020).

131 Хакерские атаки на Украину (2017). – Текст : электронный // Википедия : [сайт]. – 2017. – *URL : https://ru.wikipedia.org/wiki/Хакерские_атаки_на_Украину_(2017)* (дата обращения: 29.12.2020).

132 Спецслужбы ФРГ : вирус *Petya* позволяет красть данные. – Текст : электронный // ТАСС : [сайт]. – 2017. – *URL : https://tass.ru/mezhdunarodnaya-panorama/4396011* (дата обращения: 29.12.2020).

133 *Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops* = Изучение угроз и уязвимостей в хакерской сети / В. Бенджами, В. Ли, Т. Холт, Х. Чен. – Текст: электронный // *ResearchGate*. – 2019. – Режим доступа: для авториз. пользователей. – *URL : https://www.researchgate.net/publication/307747097_Exploring_threats_and_vul*

nerabilities_in_hacker_web_Forums_IRC_and_carding_shops (дата обращения: 08.07.2021).

134 Рынок преступных кибероуслуг 2018. – Текст. Изображение : электронные // *Positive Technologies* : [сайт]. – 2018. – *URL :* *https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Darkweb-2018-rus.pdf* (дата обращения: 11.11.2020).

135 Чои С. *A Study on Analysis of Malicious Code Behavior Information for Predicting Security Threats in New Environments* = Исследование по анализу информации о поведении вредоносного кода для прогнозирования угроз безопасности в новых средах / С. Чои, Т. Ли, Д. Квак // *KSII Transactions on Internet and Information Systems.* – 2019. – № 13 (3). – С. 1611–1625. – *DOI : https://doi.org/10.3837/tiis.2019.03.028*. – Текст : электронный (дата обращения: 08.07.2021).

136 Российская Федерация. Законы. О создании Государственной системы обнаружения и предотвращения компьютерных атак : Указ Президента РФ №31с : [подписан Президентом Российской Федерации В. Путиным 15 января 2013 года] : (редакция от 22.12.2017). – Доступ из справ.-правовой системы Гарант. – Текст : электронный.

137 Отчет центра мониторингаи реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности Банка России 1.09.2018 – 31.08.2019**.** – Текст : электронный // ФинЦЕРТ: [сайт]. – URL : *https://cbr.ru/https://www.cbr.ru/content/document/file/84354/fincert_report_20191010.pdf* (дата обращения: 17.11.2019).

138 *2021 Cyber Security Statistics* = Статистика кибербезопасности за 2021 год. – Текст. Изображение : электронные // *Purplesec :* [сайт]. – 2016. – *URL : https://purplesec.us/resources/cyber-security-statistics/#:~:text=Cyber%20Security%20Risks,and%20health%20records%20left%20unprotected* (дата обращения: 08.07.2021).

139 Материалы о *Solar JSOC.* – Текст : электронный // Ростелеком Солар : [сайт]. – *URL : https://rt-solar.ru/products/jsoc/materials/* (дата обращения: 08.07.2021).

140 Отчёт Центра мониторинга за первое полугодие 2018 года. – Текст. Изображение : электронные // Перспективный мониторинг : [сайт]. – 2018. – *URL : https://amonitoring.ru/service/security-operation-center1/mssp/quarterly-reports/2018-1_amonitoring_halfyear_report.pdf* (дата обращения: 08.07.2021).

141 Развитие информационных угроз во втором квартале 2020 года – Текст : электронный // Банк России : [сайт]. – *URL : https://securelist.ru/it-threat-evolution-q2-2020-pc-statistics/98256/https://www.xn--e1agzf.xn--*

d1acj3b/docs/specialists/reports/cisco/cisco_2018_acr_ru.pdf *(дата обращения: 20.12.2020).*

142 *Internet Security Threat Report April 2016* = Отчет об угрозах интернет-безопасности, апрель 2016 г. – Текст. Изображение : электронные // *Broadcom* : [сайт]. – 2016. – *URL :* https://docs.broadcom.com/doc/istr-21-2016-en (дата обращения: 08.07.2021).

143 *Data Breach Investigations Report 2020* = Отчет о расследовании нарушений данных 2020. – Текст. Изображение : электронные // *Verizon :* [сайт]. – 2020. – *URL :* https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf (дата обращения: 08.07.2021).

144 *McAfee Labs Threats Report, December 2018* = Отчет об угрозах *McAfee Labs*, ноябрь 2018 г. – Текст. Изображение : электронные // *McAfee* : [сайт]. – 2018. – *URL :* https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf *(дата обращения: 08.07.2021).*

145 *McAfee Labs Threats Report, November 2020* = Отчет об угрозах *McAfee Labs*, ноябрь 2020 г. – Текст. Изображение : электронные // *McAfee* : [сайт]. – 2020. – *URL :* https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-nov-2020.pdf (дата обращения: 08.07.2021).

146 Марин Э. *Product Offerings in Malicious Hacker Markets* = Предложения продуктов на рынках вредоносных хакеров / Э. Марин, А. Диаб, П. Шакариан. – Текст: электронный // *ResearchGate*. – 2016. – *URL :* https://www.researchgate.net/publication/305683169_Product_Offerings_i_Malicious_Hacker_Markets (дата обращения: 08.07.2021).

147 Тенденции, касающиеся рисков в сфере кибербезопасности 2017-2018. – Текст. Изображение : электронные // *Ponemon Institute LLC*– 2017-2018. – *URL : https://www.ibm.com/downloads/cas/ZYKLN2E3* (дата обращения: 20.12.2020).

148 2021 *First Half Data Breach Analysis* = Анализ нарушений данных в первом полугодии 2021 года. – Текст : электронный // *Identity Theft Resource Center :* [сайт]. – 2021. – Режим доступа : для авториз. пользователей. – *URL :* https://notified.idtheftcenter.org/s/resource#trendAnalysisSection (дата обращения: 08.07.2021).

149 Исследования за прошедшие годы. – Текст : электронный // *Search Inform Information Security* : [сайт]. – *URL :* https://searchinform.ru/practice-and-analytics/#research (дата обращения: 08.07.2021).

150 Аналитические отчеты. – Текст : электронный // *Positive Technologies :* [сайт]. – *URL :* https://www.ptsecurity.com/ru-ru/research/analytics/ (дата обращения: 08.07.2021).

151 Рынок преступных киберуслуг 2018. – Текст. Изображение : электронные // *Positive Technologies* : [сайт]. – 2018. – *URL : https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Darkweb-2018-rus.pdf* (дата обращения: 08.07.2021).

152 *Netscout Threat Intelligence Report* = Отчет об интеллектуальных угрозах Netscout. – Текст : электронный // *Netscout* : [сайт]. – 2020. – *URL : https://www.netscout.com/threatreport#download* (дата обращения: 08.07.2021).

153 Аналитические отчеты и статистика по инцидентам за прошедшие годы. – Текст : электронный // *Infowatch* : [сайт]. – *URL : https://www.infowatch.ru/analytics* (дата обращения: 08.07.2021).

154 *Threat Intelligence Reports* = Отчеты об угрозах. – Текст : электронный // *Check Point Research* : [сайт]. – *URL : https://research.checkpoint.com/category/threat-intelligence-reports/* (дата обращения: 08.07.2021).

155 Отчеты о деятельности Уполномоченного органа по защите прав субъектов персональных данных. – Текст : электронный // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций : [официальный сайт]. – *URL : https://rkn.gov.ru/personal-data/reports/* (дата обращения: 08.07.2021).

156 Состояние преступности. – Текст : электронный // Министерство внутренних дел Российской Федерации : [официальный сайт]. – *URL : https://xn--b1aew.xn--p1ai/reports* (дата обращения: 08.07.2021).

157 Отчет *Panda Security* "Понимание угроз 2020". – Текст. Изображение : электронные // *Panda Security:* [сайт]. – 2020. – *URL : https://www.cloudav.ru/upload/iblock/b58/PandaLabs%20-%20Threat-Insights-2020.pdf* (дата обращения: 08.07.2021).

158 2020 *Cyberthreat Defense Report* = Отчет об обороне от киберугроз за 2020 год. – Текст : электронный // *Imperva* : [сайт]. – 2020. – *URL : https://www.imperva.com/resources/infographics/Imperva-CDR-2020-infographic.pdf* (дата обращения: 08.07.2021).

159 *M-Trends* 2021 *Report* = Отчет об M-трендах за 2021 год. – Текст : электронный // *FireEye* : [сайт]. – 2021. – *URL : https://content.fireeye.com/m-trends/rpt-m-trends-2020* (дата обращения: 08.07.2021).

160 2020 *Cyber Threatscape Report* = Отчет о киберугрозах за 2020 год. – Текст : электронный // *Accenture* : [сайт]. – 2020. – *URL : https://www.accenture.com/_acnmedia/PDF-137/Accenture-2020-Cyber-Threatscape-Report.pdf#zoom=50* (дата обращения: 08.07.2021).

161 *ACSC Annual Cyber Threat Report* 2019-20 = Ежегодный отчет *ACSC* о киберугрозах 2019-20. – Текст : электронный // *Australian Cyber Security Centre* : [сайт]. – 2020. – *URL : https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2019-june-2020* (дата обращения: 08.07.2021).

162 *GTIC Monthly Threat Report November 2020* = Ежемесячный отчет GTIC об угрозах за ноябрь 2020. – Текст : электронный // *Global Threat Intelligence Center* : [официальный сайт]. – 2020. – *URL : https://hello.global.ntt/-/media/ntt/global/insights/gtic-monthly-threat-report/gtic-monthly-threat-report-november-2020.pdf* (дата обращения: 08.07.2021).

163 2020 *Trustwave Data Security Index* = Индекс безопасности данных *Trustwave* 2020. – Текст : электронный // *Trustwave* : [сайт]. – 2020. – *URL : https://www.trustwave.com/en-us/resources/library/documents/2020-trustwave-data-security-index/* (дата обращения: 08.07.2021).

164 *Sophos* 2021 *Threat Report*= Отчет *Threat Report om Sophos 2021*. – Текст. Изображение : электронные // *Sophos* : [сайт]. – 2021. – *URL : https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf* (дата обращения: 08.07.2021).

165 2020 *Crowdstrike Global Threat Report* = Отчет *Global Threat Report* от *CrowdStrike* 2020. – Текст. Изображение : электронные // *Crowdstrike :* [сайт]. – 2020. – *URL : https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf* (дата обращения: 08.07.2021).

166 *Group-IB* : Исследования киберугроз : [сайт]. – *URL : https://www.group-ib.ru/resources/threat-research.html* (дата обращения: 08.07.2021). – Текст. Изображение : электронные.

167 *BI.ZONE* — компания по стратегическому управлению цифровыми рисками : [сайт]. – *URL : https://bi.zone/ru/* (дата обращения: 08.07.2021). – Текст. Изображение : электронные.

168 *Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021 = Gartner* прогнозирует, что мировые расходы на безопасность и управление рисками превысят 150 миллиардов долларов в 2021 году : [сайт]. – *URL : https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem* (дата обращения: 08.07.2021). – Текст: электронный.

169 Определение параметров, влияющих на возможность реализации компьютерной атаки нарушителем / **Макарова О.С.**, Поршнев С.В. // Безопасность информационных технологий. — 2021. — Т. 28. № 2. — С. 6-20. (1,5 п.л. / 0,75 п.л.)

170 Computer attack`s probability function / Makarova O., Porshnev S. // Lecture Notes in Electrical Engineering. Advances in Automation II. — 2021. — Vol. 729. — pp. 560-568. (0,9 п.л. / 0,45 п.л.) (Scopus)

171 Оценивание вероятностей компьютерных атак на основе функций / **Макарова О.С.**, Поршнев С.В. // Безопасность информационных технологий. — 2020. — Т. 27. № 2. — С. 86-96. (1,1 п.л. / 0,6 п.л.)

172 Assessment of Probabilities of Computer Attacks Based on Analytic Hierarchy Process: Method for Calculating the Pairwise Comparison Matrixs Based on Statistical Information / Makarova Olga; Porshnev Sergey // 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). — 2020. — No. 9117676 — pp. 593-596. (0,4 п.л. / 0,2 п.л.) (Scopus)

173 Оценивание вероятностей компьютерных атак на основе метода анализа иерархий с динамическими приоритетами и предпочтениями / **Макарова О.С.**, Поршнев С.В. // Безопасность информационных технологий. — 2020. — Т. 27. № 1. — С. 6-18. (1,3 п.л. / 0,7 п.л.)

174 Методика формирования требований по обеспечению информационной безопасности сети IP-телефонии от угроз среднестатистического «хакера» / Макарова О.С. // Доклады Томского государственного университета систем управления и радиоэлектроники. — 2012. — Т. 1. № 25(2). — С. 64-68. (0,5 п.л. / 0,5 п.л.)

175 Determining the Choice of Attack Methods Approach / Makarova Olga // 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology. — 2021. — No. 9455072 — pp. 399-402. (0,3 п.л. / 0,3 п.л.)

176 Mathematical Model of the Computer Attack Implementation Possibility by an Intruder / Makarova Olga; Porshnev Sergey // 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). — 2021. — No. 9455045 — pp. 395-398. (0,4 п.л. / 0,2 п.л.)

177 Simulation of Computer Attack Scenarios for Industrial Robots from the Point of Intruder View / O. Makarova and M. Lihota // 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). — 2021. — No. 9455052 — pp. 474-477. (0,4 п.л. / 0,2 п.л.)

178 Моделирование непреднамеренного распространения информации пользователем / О.С. Макарова // Технические науки: проблемы и перспективы: материалы I Международной научной конференции (г. Санкт-Петербург, март 2011 г.). — 2011. — С. 99-103. (0,4 п.л. / 0,4 п.л.)

Приложение А. Присвоение категории значимости объектам критической информационной инфраструктуры в соответствии с показателями критериев значимости

Показатель		Значение показателя		
		III категория	II категория	I категория
I. Социальная значимость				
1.	Причинение ущерба жизни и здоровью людей (человек)	более или равно 1, но менее или равно 50	более 50, но менее или равно 500	более 500
2.	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов водоснабжения и канализации, очистки сточных вод, тепло- и электроснабжения, гидротехнических сооружений, оцениваемые:			
	а) на территории, на которой возможно нарушение обеспечения жизнедеятельности населения;	вся территория одного муниципального образования или одной внутригородской территории города федерального значения	выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта РФ или территории города федерального значения	выход за пределы территории одного субъекта РФ или территории города федерального значения
	б) по количеству людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек)	более или равно 50, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000
3.	Прекращение или нарушение функционирования объектов транспортной инфраструктуры, оцениваемые:			
	а) на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг;	вся территория одного муниципального образования или одной внутригородской территории города федерального значения	выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта РФ или территории города федерального значения	выход за пределы территории одного субъекта РФ или территории города федерального значения
	б) по количеству людей, для которых могут быть недоступны транспортные услуги (тыс. человек)	более или равно 50, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000
4.	Прекращение или нарушение функционирования сети связи, оцениваемые:			
	а) на территории, на которой возможно прекращение или нарушение функционирования сети связи;	вся территория одного муниципального образования или одной внутригородской территории города федерального значения	выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта РФ или территории города федерального значения	выход за пределы территории одного субъекта РФ или территории города федерального значения
	б) по количеству людей, для которых	более или равно 50,	более или равно 1000,	более или равно

	могут быть недоступны услуги связи (тыс. человек)	но менее 1000	но менее 5000	5000
5.	Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)	менее или равно 24, но более 12	менее или равно 12, но более 6	менее 6
II. Политическая значимость				
6.	Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)	прекращение или нарушение функционирования органа государственной власти субъекта РФ или города федерального значения	прекращение или нарушение функционирования федерального органа государственной власти	прекращение или нарушение функционирования Администрации Президента РФ, Правительства РФ, Федерального Собрания РФ, Совета Безопасности РФ, Верховного Суда РФ, Конституционного Суда РФ
7.	Нарушение условий международного договора РФ, срыв переговоров или подписания планируемого к заключению международного договора РФ, оцениваемые по уровню международного договора РФ	нарушение условий договора межведомственного характера (срыв переговоров или подписания)	нарушение условий межправительственного договора (срыв переговоров или подписания)	нарушение условий межгосударствен-ного договора (срыв переговоров или подписания)
III. Экономическая значимость				
8.	Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, муниципальным унитарным предприятием, государственной организацией, организацией с участием государства и (или) стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов прогнозируемого объема годового дохода по всем видам деятельности)	более 5, но менее или равно 10	более 10, но менее или равно 15	более 15
9.	Возникновение ущерба бюджетам РФ, оцениваемого:			
	а) в снижении доходов федерального бюджета, (процентов прогнозируемого годового дохода бюджета);	более 0,001, но менее или равно 0,05	более 0,005, но менее или равно 0,1	более 0,1
	б) в снижении доходов бюджета субъекта РФ (процентов прогнозируемого годового дохода бюджета);	более 0,001, но менее или равно 0,05	более 0,05, но менее или равно 0,1	более 0,1
	в) в снижении доходов бюджетов государственных внебюджетных фондов (процентов прогнозируемого годового дохода бюджета)	более 0,01, но менее или равно 0,5	более 0,5, но менее или равно 1	более 1
10.	Прекращение или нарушение проведения	более 3, но менее	более 70, но менее или	более 120

	клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом критической информационной инфраструктуры, являющимся в соответствии с законодательством РФ системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, оцениваемое среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций, (млн. единиц) (расчет осуществляется по итогам года, а для создаваемых объектов - на основе прогнозных значений)	или равно 70	равно 120	
IV. Экологическая значимость				
11.	Вредные воздействия на окружающую среду (ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосферу, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия), оцениваемые:			
	а) на территории, на которой окружающая среда может подвергнуться вредным воздействиям;	вся территория одного муниципального образования или одной внутригородской территории города федерального значения	выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта РФ или территории города федерального значения	выход за пределы территории одного субъекта РФ или территории города федерального значения
	б) по количеству людей, которые могут быть подвержены вредным воздействиям (тыс. человек)	более или равно 50, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000
V. Значимость для обеспечения обороны страны, безопасности государства и правопорядка				
12.	Прекращение или нарушение (невыполнение установленных показателей) функционирования пункта управления (ситуационного центра), оцениваемое в уровне (значимости) пункта управления или ситуационного центра	прекращение или нарушение функционирования пункта управления или ситуационного центра органа государственной власти субъекта РФ или города федерального значения	прекращение или нарушение функционирования пункта управления или ситуационного центра федерального органа государственной власти или государственной корпорации	прекращение или нарушение функционирования пункта управления государством или ситуационного центра Администрации Президента РФ, Правительства РФ, Федерального Собрания РФ, Совета Безопасности РФ, Верховного Суда РФ, Конституционного Суда РФ
13.	Снижение показателей государственного оборонного заказа, выполняемого субъектом критической информационной инфраструктуры, оцениваемое:			

	а) в снижении объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции);	более 5, но менее или равно 10	более 10, но менее или равно 15	более 15
	б) в увеличении времени выпуска продукции (работ, услуг) с заданным объемом (процентов установленного времени выпуска продукции)	более 3, но менее или равно 10	более 10, но менее или равно 40	более 40
14.	Прекращение или нарушение функционирования (невыполнения установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, оцениваемое в максимально допустимом времени, в течение которого информационная система может быть недоступна пользователю (часов)	менее или равно 4, но более 2	менее или равно 2, но более 1	более 1

Приложение В. Уровни возможностей нарушителей по реализации угроз безопасности информации

Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
Базовые возможности по реализации угроз БИ (H_1)	Имеет возможность при реализации угроз БИ использовать только известные уязвимости, скрипты и инструменты. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов. Обладает базовыми компьютерными знаниями и навыками на уровне пользователя. Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации, линий связи и обеспечивающие системы систем и сетей при наличии физического доступа к ним. Таким образом, нарушители с базовыми возможностями имеют возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов	Физическое лицо (хакер) Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем (администрация, охрана, уборщики и т.д.) Авторизованные пользователи систем и сетей Бывшие работники (пользователи)
Базовые повышенные возможности по реализации угроз БИ (H_2)	Обладает всеми возможностями нарушителей с базовыми возможностями. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, однако хорошо владеет этими средствами и инструментами, понимает, как они работают и может вносить изменения в их функционирование для повышения эффективности реализации угроз. Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз БИ и использования уязвимостей. Имеет навыки самостоятельного планирования и реализации сценариев угроз БИ. Обладает практическими знаниями о функционировании систем и сетей, ОС, а также имеет знания защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. Таким образом, нарушители с базовыми повышенными возможностями имеют возможность реализовывать угрозы, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей	Преступные группы (два лица и более, действующие по единому плану) Конкурирующие организации Поставщики вычислительных услуг связи Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ Системные администраторы и администраторы безопасности
Средние возможности по реализации угроз БИ (H_3)	Обладает всеми возможностями нарушителей с базовыми повышенными возможностями. Имеет возможность приобретать информацию об уязвимостях, размещаемую на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность приобретать дорогостоящие средства и инструменты для реализации угроз, размещаемые на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность самостоятельно разрабатывать средства (инструменты), необходимые для реализации угроз (КА), реализовывать угрозы с использованием данных средств. Имеет возможность получения доступа к встраиваемому программному обеспечению аппаратных платформ, системному и	Террористические, экстремистские группировки Разработчики программных, программно-аппаратных средств

	прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-аппаратным средствам для проведения их анализа. Обладает знаниями и практическими навыками проведения анализа программного кода для получения информации об уязвимостях. Обладает высокими знаниями и практическими навыками о функционировании систем и сетей, ОС, а также имеет глубокое понимание защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. Имеет возможность реализовывать угрозы безопасности информации в составе группы лиц. Таким образом, нарушители со средними возможностями имеют возможность реализовывать угрозы, в том числе на выявленные ими неизвестные уязвимости, с использованием самостоятельно разработанных для этого инструментов. Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей	
Высокие возможности по реализации угроз БИ (H_4)	Обладает всеми возможностями нарушителей со средними возможностями. Имеет возможность получения доступа к исходному коду встраиваемого ПО аппаратных платформ, системного и прикладного ПО, телекоммуникационного оборудования и других программно-аппаратных средств для получения сведений об уязвимостях «нулевого дня». Имеет возможность внедрения программных (программно-аппаратных) закладок или уязвимостей на различных этапах поставки ПО или программно-аппаратных средств. Имеет возможность создания методов и средств реализации угроз с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение. Имеет возможность реализовывать угрозы с привлечением специалистов, имеющих базовые повышенные, средние и высокие возможности. Имеет возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений. Имеет возможность долговременно и незаметно для операторов систем и сетей реализовывать угрозы безопасности информации. Обладает исключительными знаниями и практическими навыками о функционировании систем и сетей, ОС, аппаратном обеспечении, а также осведомлен о конкретных защитных механизмах, применяемых в программном обеспечении, программно-аппаратных средствах атакуемых систем и сетей. Таким образом, нарушители с высокими возможностями имеют практически неограниченные возможности реализовывать угрозы, в том числе с использованием недекларированных возможностей, программных, программно-аппаратных закладок, встроенных в компоненты систем и сетей	Специальные службы иностранных государств

Приложение С. Оценка ущерба от различных сценариев негативных последствий инцидентов информационной безопасности

Сценарий повреждения	Категория требований безопасности		
	«Стандартная»	«Высокая»	«Очень высокая»
Нарушение законов, постановлений или контрактов	– нарушение правил и законов с незначительными последствиями; – незначительные нарушения контракта, влекущие за собой самые незначительные штрафные санкции	– нарушение правил и законов с серьезными последствиями; – серьезные нарушения контракта с высокими договорными штрафами	– принципиальные нарушения постановлений и законов; – нарушение условий договора с возмещением ущерба
Нарушение права на информационное самоопределение	обработка ПД, которая может отрицательно повлиять на социальное положение или финансовое благополучие заинтересованных лиц	обработка ПД, которая может серьезно повлиять на социальное положение или финансовое благополучие заинтересованных лиц	обработка ПД, которая может привести к травмам или смерти соответствующих лиц или может поставить под угрозу личную свободу соответствующих лиц
Причинение вреда здоровью	не представляются возможными	нельзя полностью исключить причинение вреда здоровью человека	– возможны серьезные травмы; – ссуществует опасность для жизни и здоровья
Нарушение функционирования бизнес-процессов	– время простоя было определено заинтересованными сторонами как приемлемое; – максимально допустимое время простоя превышает 24 часа	– время простоя было определено некоторыми заинтересованными лицами как недопустимое; – максимально допустимое время простоя составляет от одного до 24 часов	– время простоя было определено всеми заинтересованными лицами как недопустимое; – максимально допустимое время простоя составляет менее одного часа
Негативные последствия, как на внутренние бизнес-процессы, так и на репутацию организации	ожидается только минимальное ухудшение или только внутреннее ухудшение репутации организации	можно ожидать значительного ухудшения репутации	возможна потеря репутации в масштабах всей страны, что может даже поставить под угрозу существование организации
Финансовые последствия	финансовые потери приемлемы для организации (не превышают 10 000 евро для малого предприятия)	финансовые потери значительны, но не угрожают существованию организации (от 10 000 до 100 000 евро)	финансовые убытки угрожают существованию организации (более 100 000 евро)

Приложение D. Научные подходы, используемые для определения и прогнозирования компьютерных атак

№ п/п	Источник	Цели исследования	Краткая информация о результатах исследования	Математический метод	Подход к оцениванию рисков ИБ
1.	Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры [56]	Разработка технологии анализа киберугроз и оценки рисков нарушения кибербезопасности энергетической инфраструктуры с применением предложенного методического подхода и разрабатываемой интеллектуальной системы	1. Предложенная методика анализа киберугроз энергетической инфраструктуры разработана в соответствии со стандартом *ISO*/МЭК 27005-2011. 2. Предложен подход формирования сценариев векторов КА представлена в виде графовой модели, описывающей причинно-следственную цепочку угроз кибернетической и энергетической безопасности, причин их возникновения, последствий, а также вероятность их наступления и степень критичности экстремальной ситуации. 3. Предлагается сценарное планирование с применением инструмента байесовских сетей доверия. Сценарии оцениваются интегральным показателем вероятности возникновения экстремальной ситуации на объекте. Данный показатель определяется экспертами. Такие ситуации рассматриваются как пессимистический сценарий – набор событий и взаимосвязей между ними, которые приводят к максимальным потерям и ущербу в результате их возникновения и развития. 4. Разработана автоматизированная интеллектуальная система по реализации методики. 5. Оценка эффективности и реалистичности предложенной методики не представлена.	Байесовские сети доверия	Оценка рисков с точки зрения организации (экспертное формирование перечня рисков) без учета изменения вектора угроз со временем
2.	Метод выбора системы защиты информации с учетом критерия конкурентоспособности предприятия [57]	Исследуется метод прогнозирования снижения ущерба от нарушения ИБ после внедрения средств ЗИ	1. Предложена методика формирования перечня рисков, основанная на подходе определения угроз ФСТЭК России 2008 года и *CVE*. 2. Предложен метод выбора средства ЗИ, приводящий к повышению состояния защищенности от угроз ИБ, используя критерий обеспечения конкурентоспособности предприятия (т.е. с минимальными затратами). 3. Подтверждение эффективности реализовано путем практической апробации метода на доном предприятии с 2009 г. по 2011 г.	Модифицированный метод рандомизированных сводных показателей	Оценка рисков и подбор средств ЗИ с точки зрения организации в соответствии с ФЗ РФ (критерий выбора – экономический) без учета изменения вектора угроз со временем
3.	Оценка информационных рисков в распределенных системах обработки	Исследование модели информационных рисков, представленной в виде взвешенного	1. Описан подход к формированию взвешенного динамического гиперграфа вершинами которого являются угрозы, уязвимости и КА, динамически возникающие в момент времени. 2. Описан подход для оценки ущерба от реализации риска от таких параметров как уровень критичности возникновения угрозы, вероятности реализации КА со стороны угрозы через определенную уязвимость с помощью	Взвешенный динамический гиперграф	Оценка рисков с точки зрения организации с учетом динамики изменения вектора КА

	данных на основе беспроводных сенсорных сетей [18]	динамического гиперграфа	взвешенного динамического гиперграфа. 3. Приведено практическое применение исследуемого метода для *SCADA* систем. 4. Оценка эффективности и реалистичности предложенной методики не представлена.		
4.	Оценка рисков в функционирующей ИС [58]	Исследование методологии оценки рисков ИБ на базе экспертной методики анализа рисков в соответствии со стандартом *ISO*/МЭК 27005-2011	1. Описан подход к оценке рисков в соответствии со стандартом *ISO*/МЭК 27005-2011. 2. Предложено использование усовершенствованного метода оценки рисков на базе методологии *OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation* — Оценка оперативной критической угрозы, активов и уязвимостей). Особенность подхода заключается в создании рабочей группы как технических специалистов, так и управленческого персонала для многосторонней оценки рисков ИБ. 3. Оценка эффективности и реалистичности предложенной методики не представлена.	Экспертные методы оценки	Оценка рисков с точки зрения организации с помощью экспертного подхода без учета изменения вектора угроз со временем
5.	*A Study on Analysis of Malicious Code Behavior Information for Predicting Security Threats in New Environments* [32]	Исследование закономерностей поведения вредоносного кода с целью прогнозирования угроз ИБ в новых средах	1. Предложен подход к анализу и группировки ВПО на основе следующих характеристик: путь заражения и распространения; тип заражения и распространения; зависимость от пользователя; цель КА; исполнитель; поведение КА. 2. Процесс оценки возможности использования групп ВПО на вновь появившиеся новой технологии или устройства на основе структуры применения ВПО, представленной выше, назван процессом расширения. – Определение исходных данных, необходимых для процесса расширения: возможности новой технологии (вычислительные возможности, сетевая функция, функция хранения, возможность соединения с другими носителями и типами данных, которые можно создавать заново и управлять ими). – Сравнение характеристик новой технологии с характеристиками группировки для определения схожести контента. – Выбор ВПО, которое может использоваться в новой технологии. 3. Оценка эффективности и реалистичности предложенной методики не представлена.	Принцип аналогии	Оценка с точки зрения нарушителя вероятности КА с помощью известного ВПО на вновь разработанное ПО
6.	*Stopping the Cyberattack in the Early Stage: Assessing the Security Risks of Social Network Users* [33]	Исследуется возможность предотвращения КА социальной инженерии на организации путем оценки защищенности сотрудников в социальных сетях	1. Предложена модель оценки защищенности предприятия от методов социальной инженерии. Сотрудник, являющийся пользователем социальной сети, рассматривается точка входа для реализации КА на организацию с помощью социальной инженерии. 2. Разработана модель, основанная на использовании для оценки ИБ пользователя в социальной сети алгоритмов машинного обучения, в которой используется социальный граф отношений пользователей. В рамках модели определяются: – предпочтения тем пользователем;	Алгоритмы машинного обучения (логическая регрессия, случайный лес, дерево решений с градиентным усилением,	Модель анализа пользователей для выявления потенциальных жертв социальной инженерии путем анализа личной информации и поведения пользователей в

			– связи с другими пользователями; – время, проведенное в социальных сетях, вовлеченность в переписку в микроблогах; – подобие пользовательского поведения; – взаимосвязи. 3. Для каждого пользователя формируются следующие показатели: – уровень активности; – вероятность обратного следования; – сложность социального круга; – частота взаимодействия; – степень очевидности предпочтений. 4. Оценка эффективности и реалистичности предложенной методики не представлена.	наивный байесовский и опорные векторные машины, теория графов)	социальных сетях без учета изменения данных со временем
7.	*Research on Privacy Security Risk Assessment Method of Mobile Commerce Based on Information Entropy and Markov* [59]	Исследование метода оценки рисков конфиденциальности ИБ мобильных устройств на основе информационной энтропии и цепей Маркова	1. Предложен метод оценки риска конфиденциальности для мобильных устройств на основе информационной энтропии и цепей Маркова состоит из следующих элементов: – метод оценки рисков, основанный на информационной энтропии; – математический метод описания реальной среды на основе цепей Маркова; – установление иерархии конфиденциальности рисков для мобильных пользователей. 2. Выбраны 24 показателя оценки риска раскрытия информации о конфиденциальности пользователей мобильной коммерции, которые разделены на 5 классов. В соответствии с иерархической структурой строится иерархическая модель атрибутов для риска раскрытия конфиденциальности 3. Для установления иерархии рисков выделены три уровня. Уровень вероятности возникновения факторов риска самого низкого уровня получается путем оценки экспертов, и значения ценности, полученный посредством обработки нормализации. 4. В результате формируется таблица с уровнями вероятности возникновения факторов риска. Чем выше уровень, тем труднее контролировать такие риски, и тем выше будет риск безопасности частной жизни. 5. Оценка эффективности и реалистичности предложенной методики не представлена.	Метод информационной энтропии, цепи Маркова, Байесовские сети доверия	Установления иерархии рисков конфиденциальности мобильных устройств с точки безопасности частной жизни для мобильных устройств и пользователей без учета изменения вектора угроз со временем
8.	*Enhancing is risk assessment through using combination vector matrix and octave*	Исследование возможностей повышения качества оценки рисков за счет использования комбинированных	1. Подложена комбинация методов *VECTOR* и *OCTAVE* для реализации процесса оценки рисков ИБ. 2. Особенность метода VECTOR заключается в представлении рисков в виде вектора, включающего значение уязвимости актива, ценности и отказоустойчивости актива, угрозы для актива и последствий от реализации угрозы, данных о требуемом уровне квалификации для предотвращения угрозы.	Экспертные методы оценки	Оценка рисков с точки зрения организации с помощью экспертного подхода без учета изменения вектора угроз со временем

	methods [60]	методов *VECTOR* и *OCTAVE*	3. Особенность метода *OCTAVE* в подходе к оценке рисков ИБ, а именно, формировании рабочей группой как технических специалистов, так и управленческого персонала, оценивающий значения вектора, описанного выше. 4. Оценка эффективности и реалистичности предложенной методики не представлена.		
9.	*An experimental evaluation of bow-tie analysis for security* [61]	Исследование возможности использования метода галстук-бабочка для оценки рисков ИБ	1. Предложен метод галстук-бабочка, основанный на построении наглядной диаграммы взаимосвязей элементов риска ИБ: источники риска ИБ, возможные последствия и прочие связанные с ним сущности, такие как мероприятия по снижению рисков ИБ. 2. Преимущества метода: обеспечивает наглядное, простое и ясное графическое представление рисков, ориентирован на средства управления ИБ, направленные на предупреждение и/или уменьшение последствий рисков ИБ, и оценку их эффективности. 3. Недостатки метода: не позволяет отображать совокупности причин, возникающих одновременно и вызывающих последствия, представление сложных ситуации в чрезмерно упрощенном виде, особенно при применении количественной оценки. 4. Оценка эффективности и реалистичности предложенной методики не представлена.	Теория графов	Упрощенное графическое представление рисков ИБ в текущий момент времени
10.	*Digital risk management for data attacks against state evaluation* [34]	Исследование рисков при реализации КА на данные	1. Разработано web-приложение для хранения и предоставления доступа к книгам и журналам в формате pdf с механизмами ИБ и логирования событий ИБ. 2. Проведен анализ КА на данное web-приложение, который показывает отличие рисков ИБ, сформированных с помощью нормативно правовой базы Индии и реальными КА. 3. Ограничения и границы применимости результатов не приведены. Также не предоставлена информация об объеме выборки и периоде тестирования.	Ориентированный ациклический граф	Оценка рисков на базе статистических данных, собранных путем аналитики КА на разработанное web-приложение
11.	Модель профиля угроз ИБ корпоративной ИС [62]	Исследуется специфика угроз ИБ для корпоративной ИС	1. Разработан профиль угроз ИБ для корпоративной ИС на основе основанная на подходе определения угроз ФСТЭК России 2008 года. В профиле угроз ИБ для корпоративной ИС выделено пять источников угроз ИБ: – пользователи ИС корпоративного типа или ИС, объединенные в единое звено управления; – сотрудники подразделений ИТ-служб, имеющие доступ к корпоративной ИС для поддержки ее работоспособности; – функциональные процессы встроенных (штатных) средств проверки работы доверенной среды загрузки компонентов ИС; – лица, обладающие возможностью доступа к системам хранения и передачи данных; – нарушение полномочий администраторами ИС и средств ЗИ. 2. Подход существенно сократил объем работ по оценки угроз ИБ при защите корпоративных ИС.	Теория графов	Формирование профиля угроз ИБ для корпоративной ИС с помощью классической методологии ФСТЭК России 2008 года

			3. Оценка эффективности и реалистичности предложенной методики не представлена.		
12.	Способы оценки угроз безопасности конфиденциальной информации для информационно-телекоммуникационных систем [19]	Исследуется специфика количественной оценки угроз ИБ информационно-телекоммуникационной системы	1. Предложена методология количественной оценки рисков ИБ в соответствии со стандартом *ISO*/МЭК 27005, где используются следующие статистические показатели: – средняя наработка информационно- телекоммуникационной системы на одну внутреннюю угрозу за определенный период, определяемая по суммарной наработке информационно- телекоммуникационной системы за определенный период и количеству внутренних угроз, проявившихся за этот же период; – средняя наработка информационно- телекоммуникационной системы на одну внутреннюю угрозу с последствиями за определенный период, определяемая по количеству угроз с последствиями за определенный период и средней величине ущерба на одну угрозу с последствиями; – суммарная величина ущерба собственнику за определенный период. 2. Объем и период сбора данных для определения статистических показателей не определен. 3. Оценка эффективности и реалистичности предложенной методики не представлена.	Использован набор статистических показателей, теория графов	Оценка рисков на основе статистических данных об угрозах ИБ, собранных в организации за определенный период времени (без учета динамики)
13.	*Mathematical model for calculation of information risks for information and logistics system* [20]	Исследуется оценка информационных рисков, возникающих при транспортировке или распределении материальных ресурсов	1. Предложена методика оценки рисков на базе теории орграфов с матрицей весов. 2. Оценка эффективности и реалистичности предложенной методики не представлена.	Орграфы, матрица весов, алгоритм Дейкстры	Оценка рисков с точки зрения организации с помощью орграфов без учета изменения во временем
14.	*Evaluation of information security in cloud computing based on the bayesian approach* [63]	Исследование оценки ИБ в облачных вычислениях на основе байесовского подхода	1. Предложена методология оценки защищенности облачных ресурсов с учетом исходных данных и фактических данных о событиях ИБ. 2. В работе проведен анализ существующих методов оценки рисков, их преимущества и недостатки, а также обоснована возможность использования байесовского подхода к оценке рисков. 3. В работе приведен пример реализации. 4. Оценка эффективности предложенной методики не представлена.	Байесовский подход	Оценка рисков ИБ на основе статистических и экспертных данных, собранных организацией, с учетом изменения вектора угроз со временем
15.	Метод обеспечения безопасной обработки ПД на основе применения	Исследование методов выявления недостоверности предоставляемых данных	1. Предложен метод автоматизированной оценки рисков внесения и обработки недостоверных ПД, основанный на применении теории искусственных нейронных сетей и теории нечетких множеств. 2. Приведен пример практического использования метода при вознаграждении участников работы распределенного реестра, основанном на системе социального кредитования в Китае.	Теория искусственных нейронных сетей, теория нечетких множеств	Оценка рисков недостоверности предоставляемых данных с точки зрения организации

	технологии блокчейн [21]		3. Оценка эффективности предложенной методики не представлена.		
16.	Алгоритм оценки значения остаточных рисков угроз ИБ с учетом разделения механизмов защиты на типы [64]	Исследуется защищенность организации с точки зрения существующих механизмов защиты	1. Предложено разделять механизмы защиты на: – Технические. Для технических механизмов защиты необходимо учитывать вероятность перехода в неработоспособное состояние с течением времени. – Организационные, которые имеют конечный срок действия в связи с изменяющимися внешними условиями. 2. Для каждого типа предложено составлять ориентированный граф, на основании которого строится система уравнений Колмогорова и определяется значение вероятностей каждого состояния. При расчетах для технических механизмов защиты, как и для любого оборудования, учитывается вероятность перехода в неработоспособное состояние с течением времени. 3. Оценка эффективности и реалистичности предложенной методики не представлена.	Марковский процесс, скрытая марковская модель, ориентированный граф	Методика оценки значения остаточных рисков угроз ИБ с точки зрения защитных механизмов с учетом изменения во времени
17.	Оценка рисков ИБ на основе метода построения матрицы [65]	Исследование оценки защищенности организации на базе матрицы Мак-Кинзи	1. Для оценки состояния защищенности ИС предложено воспользоваться принципом построения модели Мак-Кинзи. Модель представляет собой матрицу, состоящую из 9 ячеек для сравнительного анализа состояния ИС: 2. Принципы модели Мак-Кинзи: – Выбор критериев для оценки. В основе матрицы лежат два показателя: сильные стороны ИС и ее уязвимости, определяемые из анализа ИС. Не существует универсального списка показателей. – Определение важности критериев. Присвоение веса каждому фактору осуществляется на основании значимости для защиты ИС (сумма весов равна единице). – Оценка каждого из критериев по шкале от единицы (не привлекательный) до пяти (очень привлекательный). – Определение потенциала и стратегии развития ИС осуществляется путем умножения веса на оценку и суммирования полученные значения по всем факторам, в итоге получается взвешенная оценка / рейтинг состояния защищенности ИС. 3. Оценка эффективности и реалистичности предложенной методики не представлена.	Матрица Мак-Кинзи	Оценка рисков с точки зрения организации с помощью экспертной методологии без учета изменения вектора угроз со временем
18.	Разработка системы поддержки принятия решения для оценки рисков и угроз	Исследование принятия решения для оценки рисков и угроз национальной безопасности	1. Разработана автоматизированная система по оценке рисков ИБ, реализующая несколько методов оценки рисков (методика оценки рисков на основе событий, методика оценки рисков на основе показателей и общая методика оценки рисков национальной безопасности Российской Федерации) основываясь на реальных данных. 2. В разработанном прототипе системы в качестве исходных данных для анализа информации использованы данные из неструктурированных или	Метод анализа иерархий, теория графов	Автоматизация различных методик оценки рисков на базе экспертных и статистических значений

	национальной безопасности [66]		слабоструктурированных источников, состоящих из 40 сайтов и более 90 разделов по этим сайтам (федеральные и региональные сайты с открытыми данными, информационные агентства и новостные порталы, сайты с аналитической информацией и др.) – это более 600 млн. сообщений, собранных при помощи мониторинга ресурсов один раз в час. 3. В исследовании были определены три варианта развития ситуаций: – по пессимистичному сценарию (нужно выбрать дальнейшее действие, которое необходимо предпринять); – по наиболее вероятному сценарию (действие выбирается из заранее внесённых); – по оптимистичному сценарию (указывается срок выполнения определённых действий). 4. Для определения приоритетности оптимистичного и пессимистичного сценариев, сформированных на основе эталонных ситуаций, используется метод анализа иерархий. 5. Практическое применения рассмотрено только для рисков в целом: социальная, политическая, экономическая, природная и техногенная сфера. 6. Оценка эффективности и реалистичности предложенного решения не представлена.		
19.	Модель автоматизированной системы оптимизации параметров управления рисками в терминах угроз, уязвимостей и резервов [67]	Исследование возможностей группировки и оптимизации перечня угроз ИБ для упрощения подходов к ЗИ	1. Предложен метод оптимизации параметров управления рисков путем реализации метода оценки рисков во времени с обобщением угроз ИБ в определенные классы, что позволит упростить построение компонентов средства ЗИ, формируя барьеры защиты для целого класса угроз. 2. При расчете учитываются реальные данные о событиях ИБ, зафиксированные в организации. 3. Риск определяется по Гомперцу, что позволяет учесть их изменение во времени. Предложена формула расчета оптимального значения риска распространения угроз ИБ в ИС. 4. Оценка эффективности и реалистичности предложенного решения не представлена.	Метод имитационного моделирования	Оценка рисков с точки зрения организации с помощью экспертной методологии с учетом изменения вектора угроз со временем
20.	*Predicting Cyber-Events by Leveraging Hacker Sentiment* [35]	Исследуется влияние эмоциональной окраски сообщений на форумах *DarkNet* для прогнозирования КА	1. Предложен метод, который анализирует обсуждения на хакерских форумах для прогнозирования КА. Общая архитектура модели состоит из четырех основных задач: – сбор сообщений с *DarkNet*; – предварительная обработка текста и анализ настроений; – разработка модели временных рядов; – прогнозирование КА. 2. Анализ настроения реализуется с помощью следующих методов: *VADER, SentiStrenght и LIWC15*. 3. Эффективность данного метода составила 36%.	Теория Фрейда 1901 года о том, как оговорки могут выявить скрытые намерения человека, методы анализа временных	Прогнозирование вектора КА с точки зрения настроения нарушителя

				рядов	
21.	*Cyber/physical security vulnerability assessment integration* [22]	Исследование рисков ИБ на энергосистемы с помощью теории нечетких множеств	1. Предложен алгоритм оценки рисков кибербезопасности информационно-коммуникационной инфраструктуры энергосистемы на основе теории нечетких множеств. 2. В качестве лингвистических показателей введены следующие входные переменные: – возможности, намерения и цели нарушителя; – уязвимости и воздействия на систему. 3. Значение лингвистических переменных определяется экспертным путем. 4. Динамическое изменение во времени в системе не рассматривается. 5. Оценка эффективности и реалистичности предложенного решения не представлена.	Теория нечетких множеств	Оценка рисков для организаций энергетической сферы с помощью экспертной методологии без учетом изменения вектора угроз со временем
22.	Повышение безопасности систем управления *SCADA* [23]	Исследование угроз ИБ для *SCADA* систем	1. Предложено решение по защите SCADA от ключевых с точки зрения авторов угроз ИБ. 2. Оценка эффективности и реалистичности предложенного решения не представлена.	Экспертные методы оценки	Экспертная оценки рисков для *SCADA* систем без учетом изменения вектора угроз со временем
23.	Оценка рисков в телекоммуникационных системах [24]	Исследование рисков ИБ в энергетической сфере	1. Предложенная методика анализа киберугроз энергетической инфраструктуры разработана в соответствии со стандартом ISO/МЭК 27005-2011. 2. Разработана система автоматизации для оценивания рисков ИБ. 3. Оценка эффективности и реалистичности предложенного решения не представлена.	Экспертные методы оценки	Оценка рисков с точки зрения организации с помощью экспертного подхода без учета изменения вектора угроз со временем
24.	Методика количественного определения рисков ИБ [68]	Исследование показателей для количественной оценки рисков	1. Предложен метод количественной оценки рисков ИБ, с разделением риска невыполнения требований законодательства РФ и «реальной» реализации угрозы ИБ. Для оценки рисков использованы классические экспертные методологии. 2. Оценка эффективности и реалистичности предложенного решения не представлена.	Экспертные методы оценки	Оценка рисков с точки зрения организации с помощью экспертного подхода без учета изменения вектора угроз со временем
25.	Применение методологии stride для определения актуальных угроз безопасности программно-определяемых сетей [25]	Исследование угроз ИБ для *SDN* сетей	1. Предложено решение по защите *SDN* сетей от ключевых, с точки зрения авторов, угроз ИБ и меры ЗИ от них. 2. Оценка эффективности и реалистичности предложенного решения не представлена.	Экспертные методы оценки	Экспертная оценки рисков для *SDN* сетей без учетом изменения вектора угроз со временем
26.	*Realtime*	Исследование	1. Предложено оценивать риски ИБ на основе анализа влияния КА на	Теория	Оценка рисков с точки

	intrusion risk assessment model based on attack and servicedependency graphs [69]	влияния компонентов КА на сервисы организации	выходные данные графа КА и компонентов графа зависимостей сервисов организации (граф компонентов инфраструктуры организации). 2. Выделены 3 типа возможных корреляций между зафиксированными на трассировщике действиями системных сервисов и данными из базы данных об КА, организованной на уровне государства: – неявные корреляции (ищет сходство между предупреждениями используя парадигмы анализа данных); – полуявные корреляции (вводятся предварительные и постусловия для каждого шага в графе КА); – явные корреляции (сценарии КА определяются статически). 3. Ограничение подхода: стоимость ИБ оценивается путем измерения воздействия контрмер только на доступность активов. 4. Продемонстрировано, что предложенная методология позволяет в режиме реального времени при добавлении на граф зависимостей сервисов организации средств ЗИ определить и запустить меры противодействия.	графов	зрения организации в режиме реального времени
27.	*A safety/security risk analysis approach ofIndustrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtieanalysis* [26]	Исследование методологии оценки рисков ИБ для промышленных систем с помощью метода галстук-бабочка и дерева КА	1. Предложена методика анализа рисков ИБ состоящая из следующих этапов: – определение сценариев риска ИБ: методология, которая сочетает в себе метод галстук-бабочка (*БТ*) с деревом КА (*АТ*) для выявления причин и последствий, связанных с нарушением ИБ критических систем. – оценка вероятности определяется по шкале вероятности для входных событий, путем расчетов, с использованием вышеописанных методов, для выходных. Используется для принятия решений в системах обнаружения вторжений. – оценка тяжести последствий: количественная оценка потерь с точки зрения системных активов, человеческой жизни и ущерба окружающей среде, если произошло нежелательное событие. 2. Главным недостатком данной методологии является ее «объемность» и долгая реализация. 3. Оценка эффективности и реалистичности предложенного решения не представлена.	Теория графов, дерево КА	Наглядная оценка рисков с точки зрения организации с помощью экспертной методологии без учетом изменения вектора угроз со временем, применимая для простых систем
28.	*LiSRA: Lightweight Security Risk Assessment for decision support in information security* [70]	Исследование методологии оценки рисков ИБ экспертами на базе автоматизации расчетов	1. Предложена автоматизированная упрощенная методика оценки рисков ИБ (в соответствии со стандартом ИСО/МЭК 27005) для малых и средних организаций, состоящая из следующих этапов: – На первом этапе эксперты создают дерево КА, которые связаны с контролем ИБ в различных областях. – Пользователь автоматизированной системы расчета может выбрать область, в которой работает организация. Оценка рисков ИБ будет учитывать только деревья КА, относящиеся к соответствующей области. – Риск ИБ определяется из сценарных рисков, которые рассчитываются на	Древовидная структура	Оценка рисков ИБ для малых и средних организаций с помощью упрощенной экспертной методологии ИСО/МЭК 27005 без учетом изменения вектора угроз со

			основе как вероятности неблагоприятного воздействия, так и его тяжести с использованием деревьев КА. – Автоматизированная система определяет наиболее эффективные меры ЗИ. 2. Оценка эффективности и реалистичности предложенного решения не представлена.		временем
29.	*Forecasting IT security vulnerabilities – An empirical analysis* [36]	Обоснование методология прогнозирования уязвимостей ПО	1. Проведено сравнение различных методов прогнозирования и получены оценки точности, полученных прогнозов, в том числе: – методов одинарного, двойного и тройного экспоненциального сглаживания (*SES, DES* и *TES*); – методов регрессионного анализа; – методов статистического анализа объекта; – нейронные сети. 2. В статье получены оценки эффективности и подтверждение адекватности полученных результатов, однако, единый метод для всех типов ПО не выбран.	Методы прогнозирования временных рядов, нейронные сети	Прогнозирование уязвимостей ПО с учетом статистики о количестве найденных уязвимостей за прошлые периоды
30.	*Construction of information network vulnerability threat assessment model for CPS risk assessment* [37]	Исследование методологии оценки рисков ИБ для киберфизических систем (*CPS*) — информационно-технологическая концепция, подразумевающая интеграцию вычислительных ресурсов в физические сущности любого вида, включая биологические и рукотворные объекты	1. Предложена модель оценки рисков ИБ на базе методологии теории игр. Риск определяется по следующим параметрам: вероятность успешного вторжения сетевой КА; вероятность того, что компонент, в конечном итоге, выйдет из строя, если он будет атакован; фактическая потеря, вызванная отказом компонента. 2. Определение параметров осуществляется экспертным путем для конкретной организации при стратегии максимизации выгоды нарушителем и уменьшения вероятности сбоя в организации при КА. Данные для расчета определяют эксперты. 3. В данной методологии оценка рисков ИБ сочетается с фактическим методом контроля и планирования ИС, а также модель оценки угроз уязвимостей учитывает ограничения сторон-нарушителей и сторон-защитников.	Теория игр	Оценка рисков с точки зрения максимизации выгоды нарушителя и минимизации последствий для организации с помощью экспертной методологии без учета изменения вектора угроз со временем
31.	*Cybersecurity: Time Series Predictive Modeling of Vulnerabilities of Desktop Operating System Using*	Методология прогнозирования уязвимостей операционных систем (ОС)	1. Разработана прогностическая модель для трех популярных ОС, а именно: *Windows 7, Mac OS X* и ядро *Linux*, используя обнаруженные ими уязвимости, находящиеся в Национальной базе данных уязвимостей (*NVD*). 2. Обоснована целесообразность использования для прогнозирования вероятности КА модели *ARIMA (p, d, q)*.	Статические модели	Прогнозирование уязвимостей ПО с учетом статистики о количестве найденных уязвимостей за прошлые периоды

	Linear and Non-Linear Approach [38]				
32.	*Time series modeling of vulnerabilities* [39]	Методология прогнозирования уязвимостей ПО	1. На основе анализа временных рядов построены модели прогнозирования для пяти популярных веб-браузеров: *Chrome, Firefox, Internet Explorer, Safari* и *Opera*. 2. Результаты показали, что построенные модели временных рядов обеспечивают приемлемую точность прогноза при прогнозировании уязвимостей веб-браузеров.	Временные ряды	Прогнозирование уязвимостей ПО с учетом статистики о количестве найденных уязвимостей за прошлые периоды
33.	*Guidelines for Risk Assessment of Vulnerability Discovery Processes* [41]	Методология прогнозирования уязвимостей безопасности ПО	1. Рассмотрены методы, основанные на использовании однократного, двойного и тройного экспоненциального сглаживания, методологии Кростона, *ARIMA* и нейронных сетей. 2. Результаты данного исследования показывают, что оптимальная методология прогнозирования зависит от ПО или ОС. Абсолютные метрики могут точно покрывать фактическую ошибку прогнозирования и что точность прогнозирования является устойчивой в пределах двух применены метрики ошибок прогнозирования.	Методы скользящего сглаживания, регрессион-ный анализ, статистичес-кие методы, нейронные сети	Прогнозирование уязвимостей безопасности ПО с учетом статистики о количестве найденных уязвимостей за прошлые периоды
34.	*Cluster-based vulnerability assessment of operating systems and web browsers* [42]	Методология прогнозирования уязвимостей ПО	1. Предложено прогнозировать не отдельные уязвимости, но группу уязвимостей, так как обнаружение отдельных уязвимостей оказывается возможным далеко не во всех случаях (например, обнаруженная уязвимость нового типа может побудить злоумышленников осуществлять поиск аналогичных уязвимостей.) В этой связи предлагается разделить уязвимости на отдельные кластеры и проверить их независимость. Для кластеризации авторы использовали алгоритм *k*-средних, предназначенный для кластеризации номинальных входных переменных. 2. Получены оценки адекватности результатов, однако, единый метод оценки уязвимостей для всех типов ПО не найден.	Кластерный анализ	Прогнозирование уязвимостей ПО с учетом статистики о количестве найденных уязвимостей за прошлые периоды
35.	*Vulnerability prediction capability: A comparison between vulnerability discovery models and neural network models* [43]	Методология прогнозирования уязвимостей ПО	1. Проведено сравнение методов прогнозирования с помощью нейронных сетей и машинного обучения и получены оценки точности, полученных прогнозов. 2. Получены оценки эффективности и подтверждена адекватность полученных результатов, однако, единый метод для всех типов ПО не выбран.	Нейронные сети, машинное обучение	Прогнозирование уязвимостей ПО с учетом статистики о количестве найденных уязвимостей за прошлые периоды
36.	*The Effect of Dimensionality Reduction on*	Методология прогнозирования уязвимостей ПО	1. Предложено использовать метод прогнозирования уязвимостей ПО с помощью машинного обучения 2. Результаты показали, что ограничение области анализа уязвимостей ИБ	Машинное обучение	Прогнозирование уязвимостей ПО с учетом статистики о

	Software Vulnerability Prediction Models [44]		поиском только уязвимых частей программного кода (например, элементов взаимодействия с внешними системами, пользовательских интерфейсов) позволяет улучшить качество прогнозирования новых уязвимостей.		количестве найденных уязвимостей за прошлые периоды
37.	*A Review on Cybersecurity Threats and Statistical Models* [40]	Методология прогнозирования уязвимостей ПО	1. Проведено сравнение трех статистических моделей для обнаружения и прогнозирования уязвимостей ПО: *COPULA, ARIMA, GARCH*. 2. *COPULA* (копула, связка) – это совместное распределение случайных векторов со стандартными равномерными маргинальными распределениями. По результатам сравнения COPULA может успешно распознавать и сохранять структуру простой зависимости в многомерной информации о расположении времени. 3. *ARIMA* (*Autoregressive Integrated Moving Average* – Интегрированная модель авторегрессии – скользящего среднего) – подход, позволяющий прогнозировать временные ряды. Лучше всего подходит для прогнозирования переполнения буфера. 4. Метод *GARCH* (*Generalized Autoregressive Conditional Heteroscedasticity* – Обобщенная авторегрессионная условная гетероскедастичность) является расширением метода *ARCH*. Предоставляет более реальный контекст для предсказания цифровых данных.	Статистичес-кие методы	Прогнозирование уязвимостей ПО с учетом статистики о количестве найденных уязвимостей за прошлые периоды
38.	*Risk Assessment Method for Insider Threats in Cyber Security: A review* [71]	Исследование применимости методов *OCTAVE, CRAMM, FRAP* и *NIST SP800-30*	1. Проведен анализ и сравнение различных методов оценки рисков ИБ (*OCTAVE, CRAMM, FRAP* и *NIST SP800-30*). 2. *FRAP* (*The Facilitated Risk Assessment Process* – Облегченный процесс оценки рисков), предназначен для управления ИБ в быстро изменяющемся бизнесе. Большое внимание уделяется вовлеченности сотрудников организации. Прост в реализации. 3. *CRAMM* (*The Central Risk Analysis and Management Method* – Центральный метод анализа и управления рисками) 4. Приведены ограничения и преимущества каждого подхода. Наиболее эффективным подходом по мнению авторов является *NIST*, так как в отличии от остальных подходов учитывает внешние для организации базы знаний об рисках ИБ.	Метод экспертных оценок	Оценка рисков с точки зрения организации с помощью экспертной методологии без учета изменения вектора угроз со временем
39.	*Analytical Assessment of Security Level of Distributed and Scalable Computer Systems* [72]	Метод оценки рисков для распределенной КС	1. Предложен метод оценки и прогнозирования действий пользователя путем сбора и обработки данных об опасных действиях нарушителей, определения периметра компонентов ИС, потенциально подвергающихся КА, определения влияния негативных факторов на функционирование ИС. Метод предлагается использовать для выбора эффективных способов защиты ИС, минимизации потери от реализации КА. 2. При оценке рисков учитывается изменение КА во времени. Тем не менее, подобный учет времени позволяет оценить изменение вероятности успеха реализации, данной КА с течением времени, но не позволяет прогнозировать потенциальный вектор КА.	Теория автоматов	Оценка изменения риска КА с учетом инфраструктуры организации и существующих средств ЗИ во времени

			3. Получены комплексные аналитические оценки риска, позволяющие анализировать динамику процессов вторжения, динамику восстановления уровня безопасности и соответствующую динамику уровня рисков ИБ. 4. Критерии принятия решений об КА нарушителем, а также критерии выбора объекта КА не определены.		
40.	*Automatic cyber security risk assessment based on fuzzy fractional ordinary differential equations* [73]	Исследование схожести КА с работой иммунной системы человека	1. Предложен метод обнаружения рисков сетевой безопасности в режиме реального времени, основанный на нечетком дробном дифференциальном уравнении искусственного иммунитета, а также предложена количественная модель расчета риска сетевой безопасности на основе концентрации антител. Эта модель позволяет количественно рассчитать общий риск, с которым сталкивается узел, а также риск реализации конкретной КА. 2. Представлены результаты экспериментов, проведенных в лаборатории КА и защиты сетевой безопасности, в которых были использованы 40 компьютеров, подвергавшихся более 20 видов КА *(synflood, land, smurf* и *teardrop* и др.), подтверждающих возможность исключительно краткосрочного прогнозирования состояния ИБ.	Дифференци-альные уравнения с нечеткими параметрами	Оценка изменения риска КА с учетом инфраструктуры организации и существующих средств ЗИ во времени
41.	*Risk Assessment for Cyber Security of Manufacturing Systems: A Game Theory Approach* [74]	Исследование оценки рисков ИБ по методу анализа отказов и эффективности в производственной системе	1. Предложен метод количественной оценки рисков аналогичный методу анализа отказов и эффективности в производственной системе. В этом методе число критичности кибербезопасности определяет, является ли риск критическим, и тогда следует на него адекватно реагировать. Число критичности кибербезопасности зависит от двух элементов: серьезности риска, если он произойдет, и вероятности возникновения этого риска. 2. Основная стратегия, применяемая в этом методе – минимизация ущерба при минимальных затратах со стороны защитника. 3. Так как все данные для расчета определяются экспертами, таким образом метод можно отнести к экспертным методам оценки рисков ИБ.	Теория игр	Оценка рисков с точки зрения нарушителя с помощью экспертной методологии с учетом изменения во времени при рассмотрении реализации конкретной КА
42.	*Toward the automation of threat modeling and risk assessment in IoT systems* [27]	Исследование методологии оценки рисков ИБ на базе экспертной методики анализа рисков в соответствии со стандартом ИСО/МЭК 27005–2011	1. Предложена автоматизированная методика оценки рисков ИБ (в соответствии со стандартом ИСО/МЭК 27005) для *IoT*, ключевой особенностью является разработка каталоге угрозы. 2. Предложен практический пример реализации. 3. Оценка эффективности и реалистичности предложенного решения не представлена.	Экспертные методы оценки	Оценка рисков с точки зрения организации с помощью экспертной методологии без учета изменения вектора угроз со временем
43.	*New approach for threat classification and security risk estimations based on*	Исследование системы управления и корреляции событий ИБ	1. Предложена модель, названная *Viewnext-UEx*, для построения рейтинга угроз на основе числовых значений критичности угрозам, классифицируя их по различным типам. По общей степени критичности формирует первоочередные задачи по ЗИ, чтобы в первую очередь отреагировать на наиболее критические угрозы. Система ранжирует угрозы в порядке их приоритета для обработки и устранения угроз.	Машинное обучение	Выбор первостепенных мер ЗИ на основе ранжированного перечня угроз ИБ

	security event management [75]		2. Оценка эффективности и реалистичности предложенного решения не представлена.		
44.	*A simulation-based platform for assessing the impact of cyberthreats on smart manufacturing systems* [28]	Исследование имитационной модели КА на производственную инфраструктуру	1. Разработана имитационная модель с использованием *Arena® om Rockwell Automation* на производственной инфраструктуре. 2. Оценка эффективность работы производственной инфраструктуры определена следующими метриками: количество выполненных заказов (*TH*), уровень незавершенного производства (*WIP*) и время выполнения заказа (*LT*). 3. В работе ведется оценка метрик инфраструктуры от параметров КА. Средний уровень *WIP* и *LT* системы будут уменьшаться по мере увеличения количества ресурсов, доступных на каждой станции.	Теория игр	Оценка рисков для промышленных предприятий с точки зрения нарушителя с помощью экспертной методологии без учетом изменения вектора угроз со временем
45.	Organizational vulnerability of digital threats: A first validation of an assessment method [76]	Исследование применимости метода *SVIDT* для оценки вероятности угроз ИБ	1. Предложено использовать метод *SVIDT* для оценки вероятности угроз ИБ. В рамках *SVIDT* проводится создание качественной модели организации, в которой учтены ключевые процессы и ключевые сотрудники, анализ сильных и слабых сторон компонентов модели, количественная оценка уязвимостей и угроз ИБ, на экспертных оценок. Результатом метода является перечень сценариев действий при обращении к многофакторному системному анализу для стратегического управления. 2. Оценка эффективности и реалистичности предложенного решения не представлена.	Экспертные методы оценки	Оценка рисков с точки зрения организации с помощью экспертной методологии без учета изменения вектора угроз со временем
46.	*Armor PLC: A Platform for Cyber Security Threats Assessments for PLCs* [29]	Исследование уязвимостей программируемых логических контроллеров	1. Предложена модель угроз ИБ для виртуальных программируемых логических контроллеров. Уязвимости программируемых логических контроллеров разделены на 4 типа: в конфигурации; в сети; в ОС; в выводе ввода / вывода. 2. Предложен механизм выявления наличия КА в программируемых логических контроллерах путем сравнения конфигурации выходного значения с эталонными вариантами. 3. Оценки эффективности и реалистичности предложенного решения не представлена.	Экспертные методы оценки	Оценка рисков ИБ для виртуальных программируемых логических контроллеров с точки зрения организации с помощью экспертной методологии без учета изменения вектора угроз со временем
47.	*Methods of cyber security assessment in the information and telecommunications system* [77]	Исследование методологии оценки рисков ИБ с помощью модели дерева решений	1. Предложена методика оценки рисков ИБ (в соответствии со стандартом ИСО/МЭК 27005), ключевой отличительно особенностью является инструмент сценарного анализа влияния угроз ИБ на возникновение экстремальных ситуаций в инфраструктуре организации специального назначения. 2. Для оценки рисков предложено использовать дерево решений. Процесс построения дерева происходит сверху вниз и включает следующие этапы: – пустое дерево (есть только корень) и исходный набор (связанный с корнем); – получение подмножеств и создание *n* потомков корня, к каждому из которых прикладывается подмножество, полученное при разбиении множества;	Экспертные методы оценки	Оценка рисков для организаций специального назначения с точки зрения организации с помощью экспертной методологии без учета изменения вектора угроз со временем

			– рекурсивное применение процедуры, описанный на этапе выше, ко всем подмножествам. 3. Оценки эффективности и реалистичности предложенного решения не представлена.		
48.	*Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management* [78]	Исследование методологии оценки рисков ИБ	1. Предложен метод, в котором угроза определяется как «лицо или организация, которая намеревается причинить вред». При этом компоненты угрозы оцениваются на основе следующих двух критериев: – легкость КА связана с восприятием нарушителя того, насколько легко осуществить КА, и осведомленностью нарушителя об активах системы; – преимущества успешной КА характеризуют общую заинтересованность нарушителя угрозы в КА на систему: финансовая выгода, политическая выгода, другие выгоды. 2. Оценка эффективности и реалистичности предложенного решения не представлена.	Экспертные методы оценки	Оценка рисков с точки зрения нарушителя с помощью экспертной методологии без учета изменения вектора угроз со временем
49.	*Improving information security risk analysis by including threat-occurrence predictive models* [79]	Исследование методологии оценки рисков ИБ	1. Предложена методология смешанного качественно-количественного анализа рисков, которая вычисляет потенциальный риск и остаточный риск. 2. Предложена таблица перехода от качественных в количественные значения. 3. При построении модели угроз используются методы логистической регрессии и *SVM* регрессии для прогнозирования вектора угроз. 4. Оценка эффективности и реалистичности предложенного решения не представлена.	Экспертные методы оценки	Оценка рисков с точки зрения организации с помощью экспертной методологии с учетом изменения вектора угроз со временем
50.	*Formalization of Attack Prediction Problem* [80]	Исследование методологии оценки рисков ИБ	1. Предложена методика оценки рисков ИБ (в соответствии со стандартом ИСО/МЭК 27005), ключевой отличительно особенностью является рассмотрение мер ЗИ при оценке рисков. 2. Оценка эффективности и реалистичности предложенного решения не представлена.	Экспертные методы оценки	Оценка рисков с точки зрения организации с помощью экспертной методологии с учетом изменения вектора угроз со временем
51.	*A Data-Driven Approach to Cyber Risk Assessment* [81]	Исследование методологии оценки рисков ИБ	1. Предложена автоматизированная методика оценки рисков ИБ с учетом величины экономических потерь. 2. Оценка эффективности и реалистичности предложенного решения не представлена.	Численное моделирование	Оценка рисков с точки зрения организации с помощью экспертной методологии с учетом изменения вектора угроз со временем
52.	*Network security risk analysis using attacker's behavioral parameters* [82]	Исследования мотивов нарушителя ИБ	1. Предложена модель оценки угроз ИБ с точки зрения нарушителя. Определена мотивация нарушителя с целью определения вероятности угроз ИБ, как реализация КА с помощью наиболее вероятного пути, с точки зрения достижения цели, получения большего числа полезной информации, минимальных затрат и большего поражения цели. 2. Метод классифицирует нарушителей на четыре группы: в первую группу	Численное моделирование	Оценка рисков с точки зрения нарушителя с помощью экспертной методологии без учетом изменения вектора угроз со

			входят нарушители с целью нанесения ущерба сетевой инфрструктуре. Во вторую группу входят нарушители, имеющие некоторое ограничение в доступных ресурсах и времени. В третью группу входят нарушители, целью которых является обнаружение полезной информации. Четвертая группа состоит из нарушителей с минимальными ресурсами. 3. Данные для расчета определяются экспертами ИБ, т.е. организацией. 4. Оценка эффективности и реалистичности предложенного решения не представлена.		временем
53.	*Survey of Attack Projection, Prediction, and Forecasting in Cyber Security* [83]	Исследование сравнения методов оценки рисков	1. Проведено рассмотрение наиболее часто встречающихся методов оценки рисков: – Граф КА (часто сокращенно *AG*). Начальное состояние представляет собой состояние перед началом КА. Переходные отношения представляют собой возможные действия нарушителя. Они обычно взвешиваются, например, по вероятности того, что нарушитель выберет действие. Популярным подходом является использование интеллектуального анализа данных для создания графов КА. – Байесовская сеть - это вероятностная графическая модель, представляющая переменные и отношения между ними. Сеть представляет собой направленный ациклический граф с узлами в виде дискретных или непрерывных случайных величин и ребрами в виде отношений между ними. Каждый узел представляет переменную, имеющую определенный набор состояний. Ребра представляют причинно-следственные связи между узлами. – Теория игр - это математический инструмент, предназначенный для анализа взаимодействия субъектов с часто конфликтующими объектами. Основные допущения теории игр состоят в том, что участники рациональны (они преследуют свои цели) и что они рассуждают стратегически (они принимают во внимание свои знания или ожидания других участников). – Машинное обучение - нейронные сети, состоящие из двух этапов-обучения и тестирования. На этапе обучения изучаются соответствующие примеры из обучающего набора данных. На этапе тестирования новые данные обрабатываются моделью, и метод машинного обучения дает результаты, такие как предсказанные продолжения последовательностей КА. Однако на практике между обучением и тестированием также существует фаза валидации. На этапе валидации другой набор данных используется для оценки того, насколько хорошо была обучена модель или какие из моделей следует использовать для тестирования. 2. В статье не представлен сравнительный анализ методов и их эффективное прикладное применение.	Теория графов, Байесовские сети, машинное обучение, Теория игр	Прогнозирования векторов КА
54.	*Database intrusion*	Исследование профиля	1. Предложена методика оценки рисков на основе поведения ролей и пользователей, путем обучения системы для формирования вектора поведения	Машинное обучение	Обнаружение КА

	detection using role and user behavior based risk assessment [84]	пользователя	пользователя и обнаружения аномалий поведения. 2. Этап обучения состоит из трех этапов: – обучение на ролевом уровне (изучаются журналы транзакций, регистрации событий) для построения вектора набора поведения пользователя (*UBS*); – обучение на уровне пользователя (заключается в изучении функций из журналов транзакций, которые являются уникальными для пользователя). Эти функции затем используются на этапе обнаружения, чтобы решить, насколько близко запросы входящих транзакций напоминают прошлое поведение пользователя; – временное обучение (среднее время транзакции пользовательских транзакций можно использовать в качестве эталона для измерения временного смещения входящей транзакции с обычным поведением пользователя.) 3. Этап обнаружения в свою очередь состоит из следующих этапов: – обнаружение аномалий уровня роли (заключается в оценке последовательностей чтения / записи, возникающих в результате запросов во входящей транзакции, в сравнении с правилами зависимости данных, полученными на этапе обучения для атрибутов, присутствующих во входящем запросе); – обнаружение аномалий на уровне пользователя (этот модуль направлен на количественную оценку близости текущего поведения пользователя (извлеченного из входящей транзакции) к поведению пользователя, захваченному модулем *ULL (User Level Learning)*); – обнаружение временных аномалий (интуитивная эвристика для использования анализа времени при обнаружении вредоносных запросов заключается в простом использовании линейного расстояния временной метки входящей транзакции и среднего времени транзакции). 4. Оценка эффективности и реалистичности предложенного решения не представлена.		
55.	*A risk and security assessment of VANET availability using attack tree concept* [85]	Исследуется применимость метода уточнений *VANET*	1. Предложена методика разработки дерева КА для оценки вероятности каждого сценария КА. В данном методе дерево КА будет использовано для интерпретации КА, которые внешний нарушитель или внутренний нарушитель может генерировать в коммуникационной сети. Деревья КА позволяют измерять риски ИБ, с которыми сталкивается система в отношении потерь, вызванных КА, или выгоды защитников за счет использования мер ЗИ. 2. Продемонстрировано, что данный подход позволяет определить этапы КА. 3. Оценки эффективности и реалистичности предложенного решения не представлены.	Дерево КА	Оценки рисков с точки зрения методов реализации КА без учета изменения во времени
56.	Основные	Исследование	1. Предложены к рассмотрению несколько моделей оценки рисков ИБ.	Экспертные	Оценка рисков с точки

	подходы к анализу и оценке рисков ИБ [86]	различных методологий оценки рисков ИБ	Модель Клементса-Хоффмана строится исходя из постулата, что система ИБ должна иметь, по крайней мере, одно средство для обеспечения ИБ на каждом возможном пути воздействия нарушителя на ИС. 2. Проведен анализ методов анализа и оценки рисков: *CRAMM, CORAS, MSAT, RiskWatch* и ГРИФ. Выделены преимущества и недостатки каждого из методов.	методы оценки, Теория графов	зрения организации с помощью экспертной методологии без учетом изменения вектора угроз со временем
57.	Оценка риска: экспертный метод [87]	Исследование методов экспертной оценки рисков ИБ	1. Рассмотрены 2 подхода к экспертной оценке: – коллективная работа экспертной группы; – получение индивидуального мнения каждого из членов экспертной группы. 2. Коллективная работа экспертной группы предполагает формирование общего мнения в ходе совместного обсуждения последствий какой-либо проблемы. При коллективной работе экспертов применяются такие методы получения мнений экспертов как: «мозговая атака», деловые игры, совещания и т. д. 3. Получение индивидуального мнения членов экспертной группы предполагает получение информации от каждого из экспертов по отдельности, с последующей отработкой полученных данных. К данному способу можно отнести методы анкетирования, интервью, метод Дельфи.	Экспертные методы оценки	Оценка рисков с точки зрения организации с помощью экспертной методологии без учетом изменения вектора угроз со временем
58.	Исследование механизмов распространения запрещенного содержимого в *DarkNet* [88]	Исследуются механизмы борьбы с запрещённым контентом	1. Предложено ПО для сбора информации о механизмах получения запрещенного контента. 2. Проведен сбор информации с сайтов *DarkNet*. Общее количество пользователей на сайте 882381. Среди них 8408 пользователей, которые публиковали запрещённый контент на форуме. 43126 пользователей проявляли активность в виде написания комментариев к этому контенту. Общие количество тем на форуме 34485. 3. Определены текущие проблемы по блокировки запрещенного контента.	Численные методы	Анализ запрещенного контента
59.	*A review of cyber security risk assessment methods for SCADA systems* [30]	Исследование угроз ИБ для *SCADA* систем	1. Проанализированы особенности АСУ ТП систем с точки зрения оценки рисков ИБ и подходов к реализации мер ЗИ. 2. Оценка эффективности и реалистичности предложенного решения не представлена.	Экспертные методы оценки	Оценка рисков ИБ для АСУ ТП с точки зрения организации с помощью экспертной методологии без учета изменения вектора угроз со временем
60.	An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System [31]	Исследование методологии оценки рисков ИБ для киберфизических систем (*CPS*)	1. Проведен анализ специфики киберфизических систем (*CPS*) с точки зрения оценки рисков ИБ. 2. Рассмотрены стандарты *NERC CIP, NIST, NIPP*. 3. Оценка эффективности и реалистичности предложенного решения не представлена.	Экспертные методы оценки	Оценка рисков с точки зрения организации с помощью экспертной методологии без учета изменения вектора угроз со временем

Приложение Е. Расчет тяжести наказания за преступления

Статья /пункт	Описание пунктов статьи УК РФ	Наказание	Тяжесть наказания в терминах ожидаемой полезности
Статья 272. Неправомерный доступ к компьютерной информации			
п.1	Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, - Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.	наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.	$F_j = 24 \cdot \left(W_j + W_m \right)$
п.2	То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.	наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.	$F_j = 48 \cdot \left(W_j + W_m \right)$
п.3	Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, -	наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.	$F_j = 60 \cdot \left(W_j + W_m \right)$
п.4	Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, -	наказываются лишением свободы на срок до семи лет.	$F_j = 84 \cdot \left(W_j + W_m \right)$
Статья 273. Создание, использование и распространение вредоносных компьютерных программ			
п.1	Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, -	наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.	$F_j = 66 \cdot \left(W_j + W_m \right)$

п.2	Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, -	наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.	$F_j = 108 \cdot \left(W_j + W_m \right)$
п.3	Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, -	наказываются лишением свободы на срок до семи лет.	$F_j = 84 \cdot \left(W_j + W_m \right)$
Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей			
п.1	Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, -	наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.	$F_j = 24 \cdot \left(W_j + W_m \right)$
п.2	Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, -	наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.	$F_j = 60 \cdot \left(W_j + W_m \right)$
Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации			
п.1	Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации, -	наказываются принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.	$F_j = 96 \cdot \left(W_j + W_m \right)$
п.2	Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации	наказывается принудительными работами на срок до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет и с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до шести лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.	$F_j = 108 \cdot \left(W_j + W_m \right)$

п.3	Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации,	наказывается принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового либо лишением свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.	$F_j = 108 \cdot \left(W_j + W_m \right)$
п.4	Деяния, предусмотренные частью первой, второй или третьей настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения,	наказываются лишением свободы на срок от трех до восьми лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.	$F_j = 132 \cdot \left(W_j + W_m \right)$
п.5	Деяния, предусмотренные частью первой, второй, третьей или четвертой настоящей статьи, если они повлекли тяжкие последствия,	наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.	$F_j = 180 \cdot \left(W_j + W_m \right)$

Приложение F. Методы компьютерных атак, обсуждаемые в сети *DarkNet*

Наименование КА (угрозы)	Возможности, предоставляемые нарушителям	Доля предложений (объявлений)	Средняя стоимость на теневом рынке
Продажа ВПО:			
Криптомайнеры	проникновение на личные или корпоративные устройства и незаметное использование их вычислительных мощностей для добывания криптовалюты	20%	80$
Инструменты нарушителя	– проведение КА на сайты; – массовые почтовые рассылки; – генерация адресов и паролей; – упаковка и шифрование исполняемых файлов	19%	190$
ВПО для создания ботнета	взлом и заражение устройств, и их объединение в единую сеть	14%	700$
Трояны-вымогатели (*ransomware*)	блокировка доступа к КС или предотвращение считывания записанных в нем данных (часто с помощью методов шифрования) с дальнейшим требованием от жертвы выкупа для восстановления исходного состояния	12%	270$
RAT-трояны (троянские программы для удаленного доступа)	– слежка за действиями пользователей; – запуск файлов и выполнение команд; – запись снимков экрана; – включение веб-камеры и микрофона; – сканирование локальной сети; – загрузка файлов из интернета	12%	490$
Трояны для кражи данных (*stealer*)	– кража паролей из буфера обмена; – перехват нажатий клавиш и сохранение заголовка окна, в котором эти клавиши нажимались; – обход или отключение антивирусов; – отправка файлов на почту нарушителя	11%	100$
ВПО для *DDoS*	обрушение сервера массовой спам-атакой	5%	260$
Трояны-загрузчики (*loader*, *dropper*)	– скрытная инсталляция троянских программ и вирусов; – защита от детектирования известных ВПО антивирусами, поскольку не все из них в состоянии проверить все компоненты внутри подобных троянцев	4%	500$
ВПО для банкоматов.	несанкционированная выдача денег из банкоматов	3%	4900$
Продажа эксплойтов:			
Эксплойты	используя уязвимости в ПО, эксплоиты позволяют провести КА на КС	38% – *Windows*; 33% – веб-сервисы 19% – кроссплатформенные технологии (*Java*, *Adobe Flash*); 5% – *iOS*; 5% – *macOS*;	2540$

Продажа данных:			
Учетные данные пользователей	наиболее ценны для нарушителя: – логины и пароли пользователей платежных систем, онлайн-банков и криптовалютных бирж; – пароли от популярных онлайн-магазинов (т.к. к ним часто привязаны банковские карты). Данные позволяют совершать покупки за чужой счет, или используются торговые площадки для того, чтобы обналичить деньги с украденных банковских карт путем покупки товаров от чужого имени и их дальнейшей перепродажи	59%	<10$
Данные банковских карт	Используют для получения денег следующими способами: – покупая и продавая товары в интернете; – обналичивая средства через платежные системы; – изготавливая дубликаты банковских карт, которые потом можно использовать при снятии наличных денег из банкомата	24%	9$
Скан-копии личных и конфиденциальных документов	– документы, удостоверяющие личность, содержащие персональные данные, – паспорта, водительские удостоверения, ИНН, СНИЛС и т.п.; – финансовые документы, в том числе отчеты о кредитной истории граждан; – скан-копии внутренних документов коммерческих организаций	17%	2$

Продажа доступов, т.е. сведений, с помощью которых можно осуществить несанкционированный доступ к сайту или серверу с последующей возможностью загрузки файлов или выполнения команд.				
Доступы	– доступ к новостному сайту для распространения ВПО с его страниц и заражения посетителей; – доступ к сайту интернет-магазина для кражи данных банковских карт клиентов; – доступ к сайтам госучреждений для *DDoS* КА или дефейсу (изменению содержимого главной страницы ресурса); – доступы к серверам и рабочим станциям для распространения трояновшифровальщиков, а также в качестве точек входа в корпоративные ИС при проведении целевых КА	40% – *WebShell* 33% – *RDP* 22% – *SSH* 5% – *FTP*		
Продажа услуг				
Распространение ВПО	доставка ВПО на компьютеры жертв различными способами: – в виде вложения в фишинговых письмах; – через ссылку на скачивание файла в фишинговых письмах, SMS, сообщениях в мессенджерах и социальных сетях; – в виде поддельных файлов якобы с обновлениями или утилитами, которые размещают на взломанных или подконтрольных нарушителю сайтах; – через ботнет	28%	51%	
Разработка ВПО	преступники модифицируют методы КА, ищут новые пути обхода средств защиты и более выгодные схемы преступлений		25%	500$
Обфускация ВПО	приведение исполняемого кода с сохранением функциональности к виду, затрудняющему анализ, в частности чтобы итоговый исполняемый файл не детектировался большинством популярных антивирусов		24%	20$
Аренда инфраструктуры	– аренда выделенных серверов; – *VPN*-сервисы; – *SOCKS*5-прокси; – услуги системного администратора; – регистрация доменных имен	26%		80$
Услуги ботнета	выполнение определенных действий по команде из единого центра управления	16%		Ботнет из 1000 компьютеров – 2000$ в месяц

Дропы, обналичивание и инсайдеры	– переводы средств через платежные системы для хищения денежных средств с привязанных к аккаунтам платежных систем банковских карт пользователей; – обналичивание через сообщников в финансовых организациях; – услуги дропов – подставных лиц, которые за определённую плату выполняют «грязную» работу вроде снятия денег из банкомата с дубликатов карт, регистрации на свое имя юридического лица, получения и пересылки почтовых отправлений и т. п.	10%	20% от суммы
Взлом	– доступ к электронной почте – автоматически позволяет получить контроль над всеми личными кабинетами пользователя на различных сайтах, где данная почта использовалась для регистрации аккаунта; – доступ к сайтам, серверам, сетевому оборудованию	7%	• 50$ • 200$
Спам-рассылки	– Спам-рассылка по электронной почте; – Спам-рассылка в мессенджерах; – Рассылка ВПО по электронной почте; – Спам-рассылка по *SMS*	3%	1$/ 1000 писем
Услуги *DDoS*	цели КА: вымогательство и похищение данных, влияние на ход выборов в других странах, конкуренция в бизнесе («подстава» в период активных продаж) и т.д.	2%	КА на сайт мощностью 270 Гбит/с 50$ в сутки

Приложение G. Описание ПАК «Ampire»

В ПАК «*Ampire*» реализован типовой шаблон ИС «Организация топливно-энергетической сферы», моделирующий работу организации. В шаблон «Организация топливно-энергетической сферы» входят следующие сегменты:

- сегмент сети Интернет;
- сегмент внешнего периметра организации;
- сегмент корпоративного центра обработки данных;
- сегмент пользовательского отдела «Разработчики»;
- сегмент пользовательского отдела «Пользователи»;
- сегмент АСУ ТП.

ПАК «*Ampire*» реализует 6 сценариев автоматической реализации КА:

1. набор из 4-х сценариев действий внешнего нарушителя:
   - защита баз данных;
   - защита контроллера домена предприятия;
   - защита данных файлового сервера;
   - защита данных сегмента АСУ ТП.
2. набор из 2-х (двух) сценариев действий внутреннего нарушителя:
   - защита научно-технической информации предприятия;
   - защита корпоративного портала.

В каждом сценарии указывается виртуальный нарушитель и уязвимости, через которые он проводит КА. ПАК «*Ampire*» содержит следующие типы инструментов (но не ограничивается ими):

- *Vulnerability assessment and Penetration testing;*
- *System Information and Event Management;*
- *Firewall;*
- *Intrusion Detection and Prevention;*
- *Digital Forensics Investigation;*
- *Malware Analysis and Reverse Engineering;*

– *Incident Response.*

В сценарии ПАК «*Ampire*» включены следующие типы атак:

– *Denial of services;*
– *Network and application reconnaissance;*
– *Phishing website;*
– *Phishing Emails;*
– *Spams;*
– *Malicious website;*
– *Malicious domain;*
– *Emerging and Known Malware for Windows, OS-X, Linux, Android, iOS and IoT platforms;*
– *Exploit Kits;*
– *Server- and client-side vulnerabilities and exploits;*
– *Data Leakage;*
– *Brute-forcing;*
– *Botnet communications.*

В шаблонах ПАК «*Ampire*» могут быть реализованы следующие сервисы:

– *ICS/SCADA;*
– *Marketplaces;*
– *Cloud;*
– *Real-Time Entertainment;*
– *Gaming, Banking;*
– *Tunneling;*
– *File sharing;*
– *Hypervisor;*
– *VoIP;*
– *Webmail;*
– *Web browsing;*
– *Social networking;*

– *Productivity applications.*

Ролевая модель ПАК «*Ampire*» выглядит следующим образом: каждый пользователь принадлежит к одной из трёх категорий:

1. Администратор. Администратор отвечает за развёртывание системы и организацию пользовательской инфраструктуры ПАК «*Ampire*». Он может создавать/блокировать пользователей, назначать пользователей преподавателями, управлять шаблонами ИС (добавлять, редактировать, удалять). Администратор ПАК «*Ampire*» не имеет доступа к интерфейсу преподавателя и интерфейсу обучаемого.

2. Преподаватель. Преподаватель отвечает за проведение практических занятий по обучению методам обнаружения, анализа и устранения последствий компьютерных атак на базе ПАК «*Ampire*». Он может управлять пользователями, которые проходят обучение (создавать, редактировать и удалять профили пользователей), включать их в группы мониторинга и реагирования, создавать тренировки на базе имеющихся шаблонов. Для отработки навыков обнаружения и устранения последствий компьютерных атак преподавателю доступна возможность управления виртуальными нарушителями (запуск сценария атаки, остановка, выполнение отдельных этапов). Для оценки качества работы группы мониторинга преподаватель имеет возможность просматривать и оценивать создаваемые обучаемыми карточки инцидентов. Для выдачи рекомендаций обучаемым преподавателю доступна система быстрых сообщений (мессенджер). В процессе тренировки преподаватель может в онлайн-режиме отслеживать статусы заложенных в шаблон уязвимостей, корректность работы всех узлов ИС, на которой проходит тренировка.

Обычный пользователь (обучаемый) имеет доступ к встроенным в шаблон ИС средствам обнаружения КА, а также дополнительным системам ЗИ, характерных для выбранной тренировки. Обучаемый, выполняя роль в группе мониторинга, имеет возможность создавать карточки инцидентов и получать по ним обратную связь. При участии в группе реагирования пользователю доступна возможность непосредственного подключения узлам ИС, используемого шаблона, для проведения детального анализа инцидента и внесения изменений для устранения уязвимостей ИБ.

Приложение Н. Анализ общедоступных источников статистической информации о компьютерной атаке

№	Организация, которая ведет сбор статистики	Наименование отчета	Объем анализируемых статистических данных об инцидентах	Статистика о каком типе организаций собирается	Период сбора статистики	Периодичность публикации отчетов
1.	Финцерт – Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере, специальное структурное подразделение Банка России (РФ)	Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности банка России [137]	826 организаций (более 1000 запросов от 1100 пользователей в сутки)	Кредитно-финансовые организации	2015–2021 гг.	ежегодно
2.	*PurpleSec LLC* – поставщик услуг по ИБ (США)	2020 *Ransomware Statistics, Data, & Trends* [138]	-	Отрасли промышленности Северной Америки (правительство, строительство, производство и т.д.)	2019–2021 гг.	ежегодно, раз в полгода
3.	ООО «СОЛАР СЕКЬЮРИТИ», компания группы ПАО «Ростелеком» - коммерческий центр мониторинга (РФ)	*Solar JSOC Security Report* 2019 [139]	более 100 организаций (86,7 млрд событий в сутки)	госсектор, финансы, нефтегазовая отрасль, энергетика, телекоммуникации, крупный ритейл	2018–2019 гг.	ежегодно, квартально
4.	Перспективный мониторинг - коммерческий центр мониторинга (РФ)	Отчёт Центра мониторинга за первое полугодие 2018 года [140]	112 млн. событий	пользовательские АРМ, web-серверы, межсетевые экраны, почтовые серверы, файловые серверы	Первый квартал 2016 – первый квартал Q1 2018 гг.	раз в полгода
5.	Лаборатория Касперского (*Kaspersky Security Network*) – производитель средств антивирусной защиты (РФ)	Развитие информационных угроз во втором квартале 2020 года. Статистика по ПК [141]	726 536 269 атак	частные лица, банковская сфера, веб-сервисы	2009–2021 гг.	ежеквартально
6.	*Cisco* – производитель средств сетевой безопасности (США)	Отчет *Cisco* по информационной безопасности за 2018 год []	3600 респондентов из 26 стран	web-серверы, почтовые серверы и др.	2014–2018	ежегодно
7.	*Symantec* – производитель средств антивирусной защиты (США)	*Internet Security Threat Report* [142]	63,8 млн. событий в секунду (157 стран)	облачные серверы, почтовые серверы, web-серверы и т.п.	с 2004 г.	ежегодно
8.	*Verizon*- коммерческий центр мониторинга (США)	2020 *Data Breach Investigations Report* [143]	-	финансовый сектор, медицина, учебные учреждения	2015–2021 гг.	ежегодно

9.	*McAfee + MITER Corporation* – производитель средств антивирусной защиты (США)	*McAfee Labs Threats Report* [144, 145]	более 500 млн. потребителей	пользовательские АРМ	2016–2021 гг.	квартально
10.	*Arizona State University*– исследовательский университет (США)	*Product Offerings in Malicious Hacker Markets* [146]	431 518 сообщений в 101 711 темах, написанных 40 372 авторами	17 рынков в *DarkNet*	ноябрь 2004 – сентябрь 2015 гг.	-
11.	*Ponemon Institute LLC* – исследовательский университет (США)	*Cost of Data Breach Study* [147]	419 организаций в 13 странах	бизнес сектор, пользовательские АРМ	2017–2018 гг.	ежемесячно, ежегодно
12.	*Identity Theft Resource Center* – некоммерческая организация (США)	[148]	-	ведущие некоммерческие, медицинские и образовательные учреждения	2005–2021 гг.	ежемесячно, ежегодно
13.	ООО «СёрчИнформ» - производитель средств ЗИ (РФ)	Инциденты внутренней безопасности в российских компаниях. Данные за первое полугодие 2020 года [149]	-	Банки, государственные и образовательные учреждения, страховые компании, вооруженные силы, здравоохранение	2016–2021 гг.	ежемесячно, ежегодно
14.	*Positive Technologies* - производитель средств ЗИ (РФ)	Актуальные киберугрозы за II квартал 2020 года Рынок преступных киберуслуг 2018 [150, 151]	25 наиболее популярных англоязычных и русскоязычных теневых торговых площадок, с общим числом зарегистрированных пользователей более трех миллионов. Эксперты *Positive Technologies* исследовали более 10 000 предложений теневого рынка киберуслуг. На рынке представлено более 50 различных категорий товаров и услуг, которые в совокупности могут быть использованы для организации любой изавестной на сегодняшний день КА		2012–2021 гг.	ежеквартально
15.	*Netscout*- коммерческий центр мониторинга (США)	*NETSCOUT THREAT INTELLIGENCE REPORT* [152]	-	здравоохранение и образовательные услуги	2019–2021 гг.	ежеквартально
16.	*InfoWatch*- производитель средств ЗИ (РФ)	*COVID*-19: утечки периода пандемии (1 полугодие 2020 г.) [153]	-	финансовая сфера, интернет сервисы, частные лица, медицинская сфера	2017–2021 гг.	ежеквартально
17.	*Check Point Research* – производитель средств сетевой безопасности (Израиль)	[154]	-		2017–2021 гг.	еженедельно
18.	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций - уполномоченный орган по защите прав субъектов ПД (РФ)	[155]	-	операторы ПД	2009–2021 гг.	ежегодно
19.	Министерство внутренних дел РФ -	[156]		юридические лица РФ	2019–2021	ежемесяч

	административно-распорядительные функции в сфере обеспечения общественной безопасности, охраны правопорядка, борьбы с преступностью (РФ)				гг.	но
20.	*Panda Security* - производитель средств ЗИ (Испания)	Понимание угроз 2020 [157]	-	все типы	2017–2021 гг.	раз в 1,5 года
21.	*Imperva* - производитель средств ЗИ (США)	2020 *Cyberthreat Defense Report* [158]	ответы от 1 200 квалифицированных специалистов и практиков ИБ из организаций с более чем 500 сотрудников из 17 стран Северной Америки, Европы и Азии	финансы, розничная торговля, телекоммуникации и технологии, образование, здравоохранение, промышленность, правительственная сфера	2017–2021 гг.	ежегодно
22.	*FireEye*- производитель средств ЗИ (США)	*M-Trends 2020 Report* [159]	1,1 млн образцов в день за 2019 год	аэрокосмическая промышленность / оборона, биотехнологии, бизнес/профессиональные услуги, строительство/инженерное дело, образование, энергия, развлечения/средства массовой информации, финансы, правительство, здравоохранение, высокие технологии, некоммерческая, розничная торговля/гостеприимство, телекоммуникации, транспорт/логистика, утилиты	2010–2021 гг.	ежегодно
23.	*Accenture* – аудиторская организация (Ирландия)	2020 *Cyber Threatscape Report* [160]	-	организации в сферах стратегического планирования, оптимизации и организации аутсорсинга бизнес-процессов, управления	2016–2021 гг.	ежегодно

				взаимоотношениями с клиентами, управления логистическими процессами, управления персоналом, внедрения информационных технологий		
24.	Австралийский центр кибербезопасности (ACSC) – государственный центр мониторинга инцидентов ИБ (Австралия)	*ACSC Annual Cyber Threat Report, July 2019 to June 2020* [161]	2266 инцидентов кибербезопасности и 59806 отчетов о киберпреступлениях	государственный сектор, образование, банковская и финансовая сфера, информационные технологии, здравоохранение, розничные продажи, коммуникации, транспорт Австралии	2015–2021 гг.	ежегодно
25.	*Nippon Telegraph and Telephone* – сервис провайдер ИБ (Япония)	*Monthly Threat Report November* 2020 [162]	-	финансы, технологии, бизнес и профессиональные сервисы, образование, государственный сектор Японии	2017-2021 гг.	ежемесячно
26.	*Trustwave Holdings* – сервис провайдер ИБ (Сингапур)	2020 *Trustwave Data Security Index* [163]	-	розничная торговля, финансы Сингапура	2010-2021 гг.	ежегодно
27.	*Sophos* - производитель средств ЗИ (Великобритания)	*SOPHOS 2021 THREAT REPORT* [164]	-	-	2005–2021 гг.	ежегодно
28.	*CrowdStrike Holdings, Inc*. – сервис провайдер ИБ (США)	*2020 CrowdStrike Global Threat Report* [165]	более 35 000 инцидентов ИБ	местное управление и муниципалитеты, академическая сфера, технологии, здравоохранение, обрабатывающая промышленность, финансовая сфера, СМИ	2014–2021 гг.	ежегодно
29.	*Group-IB* – сервис провайдер ИБ (РФ)	*HI-TECH CRIME TRENDS* 2019/2020 [166]	-	телекоммуникационный сектор, Энергетический сектор, Финансовый сектор	2015-2021 гг.	ежегодно
30.	*BI.ZONE* – сервис провайдер ИБ (РФ)	*Threat Zone* 2020 [167]	-	банки, интернет-сервисы, веб-сервисы, сотовые операторы	2018–2021 гг.	ежегодно
31.	*Tadviser* – новостной агрегатор	Статья:Потери_банков_от_киберпреступности [105]	-	Банки	2016-2021гг.	По мере появления публичной информац

						ии (ежедневно)
32.		Статья:Киберпреступность_и_киберконфликты_:_Россия [104]	-	-	2016-2021гг.	По мере появления публичной информации (ежедневно)