МЕТОДИЧЕСКИЕ АСПЕКТЫ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

METHODOLOGICAL ASPECTS OF RESPONDING TO INFORMATION SECURITY INCIDENTS IN THE DIGITAL ECONOMY

УДК 004.056 + 338.46.
DOI: 10.25631/PEJ.2020.1.155.162

МАЙОРОВА Елена Витальевна
доцент кафедры вычислительных систем и программирования Санкт-Петербургского государственного экономического университета, кандидат технических наук, chertok83@mail.ru

MAYOROVA, Elena Vitalievna
Associate Professor at the Department of Computer Systems and Programming, Saint Petersburg State University of Economics, Candidate of Technical Sciences, chertok83@mail.ru

Аннотация.
В статье рассмотрены проблемы информационной безопасности, сопровождающие процессы цифровизации экономики и других областей профессиональной деятельности. Рассмотрены виды кибератак на информационные системы организаций и проанализирован ущерб, причиненный организациям в результате реализации инцидентов информационной безопасности. Предложены методы реагирования на инциденты информационной безопасности. Определены источники данных для расследования инцидентов. Приводятся рекомендации использования специализированного программного обеспечения в качестве источника данных для расследования инцидентов и снижения рисков.

Ключевые слова: информационная безопасность, программное обеспечение, инцидент информационной безопасности, кибератака, потери от реализации угроз информационной безопасности, риск.

Abstract.
The article deals with the problems of information security that accompany the processes of digitalization of the economy and other areas of professional activity. The types of cyber attacks on organizations information systems are considered and the damage caused to organizations as a result of information security incidents is analyzed. Methods for responding to information security incidents are proposed.

Data sources for investigating incidents have been identified. Recommendations for using specialized software as a data source for investigating incidents and reducing risks are given.

Key words: information security, software, information security incident, cyber attack, losses from the implementation of is threats, risk.

По данным международных экспертов по кибербезопасности Cybersecurity Ventures, в 2019 г. кибератаки происходили каждые 14 секунд по всему миру [1; 2]. Увеличение числа кибератак приводит к увеличению причиняемого ими ущерба. Например, только потери от мошенничества с онлайн-платежами в 2018 г. составили 22 млрд долл. Так, в 2018 г. международные компании различных секторов экономики потерпели убытки более 3 трлн долл. Согласно прогнозу Всемирного экономического форума, в 2022 г. сумма общего ущерба организаций всего мира от кибератак может достигнуть 8 трлн долл. [2].

В 2016 г., по данным FinCERT (подразделение Центрального банка Российской Федерации по борьбе с кибермошенничеством), ущерб компаний в результате кибератак составил около 1,6 млрд руб., ущерб банков – более 2 млрд руб.

Эксперты по информационной безопасности (ИБ) российской компании «Positive Technologies» предполагают, что количество кибератак на все финансовые системы может вырасти на 30% в течение последующих лет [3].

Согласно исследованию, проведенному специализированной международной компанией Global Emergency Response Team (GERT), работающей в сфере цифровой криминалистики и реагирования на инциденты ИБ (далее инциденты), и ее подразделения, занимающиеся реагированием на инциденты и исследованиями вредоносного программного обеспечения (ПО) Global Research and Analysis Team (GReAT) [4], заметили, что наибольшая доля целевых кибератак приходится на финансовые организации (рисунок 1).

В рамках этого же исследования [4; 5] отмечается, что большая часть обращений по расследованиям инцидентов связана с обнаружением последствий кибератаки (несанкционированный перевод денежных средств, зашифрованные рабочие станции, недоступность цифровых сервисов и т. п.), что указывает на необходимость совершенствования методов обнаружения кибератак и оптимизации процессов реагирования на инциденты. Это позволило бы избежать финансовых потерь и свести к минимуму ущерб от атак на инфраструктуру компаний.

Наиболее частой причиной обращения для расследования инцидентов является атака шифровальщиков (рисунок 2). Данная категория атак характеризуется высокой скоростью развития и сложно определяется на ранних стадиях, при этом приводит к блокировке доступа к компьютерной системе, что влечет за собой значительные финансовые потери.

Так ПАО «Сбербанк» в своем годовом отчете за 2018 г. среди ключевых мероприятий на 2020 г. отмечает включение ИТ-продуктов блока «Риски» в периметр Agile-трансформации [6]. Среди прочих рисков ПАО «Сбербанк» выделяет такие риски, как операционный риск, правовой риск и риск кибербезопасности. К операционному риску относятся следующие категории событий информационной системы банка, его порождающие (рисунок 3).

Операционный риск является риском возникновения потерь вследствие недостатков (уязвимостей) во внутренних процессах, в функционировании информационных систем организации, несанкционированных или противоправных действий, ошибок сотрудников или вследствие внешних событий. В рамках политики управления операционными рисками предлагается комплекс мер,

Рисунок 1
Доля целевых кибератак на организации различных областей профессиональной деятельности в 2018 г. [5]

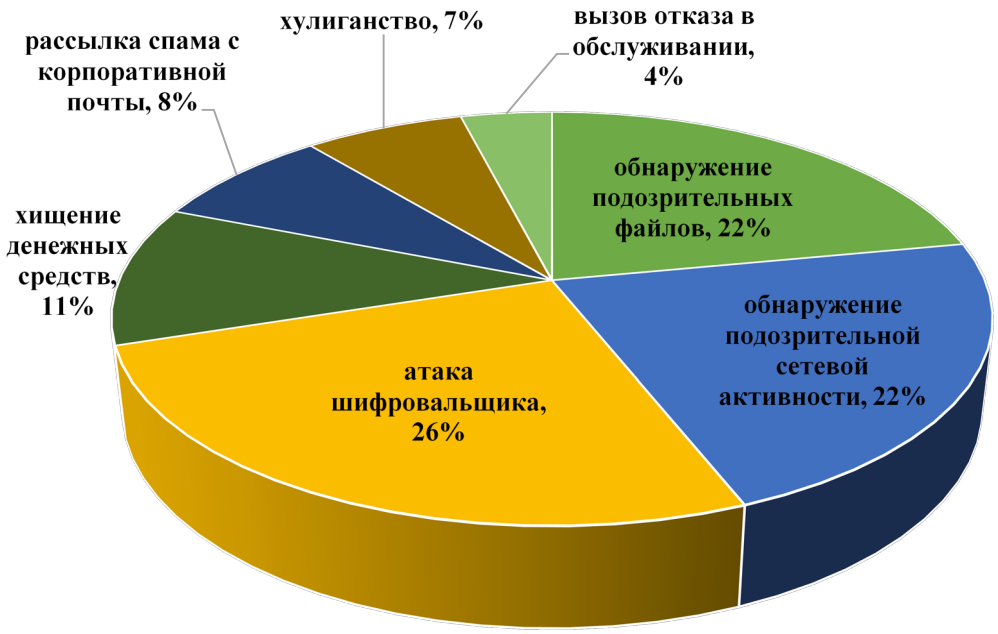

Рисунок 2
Виды атак на инфраструктуру организаций в 2018 г. [5]

направленных на обеспечение ИБ и непрерывность деятельности организации. Комплекс мер по идентификации операционного риска представлен на рисунке 4.

Анализ данных о возникновении операционного риска и понесенном ущербе указывает на то, что все организации, вне зависимости от отраслевой и территориальной принад-

Рисунок 3
События операционного риска Сбербанка

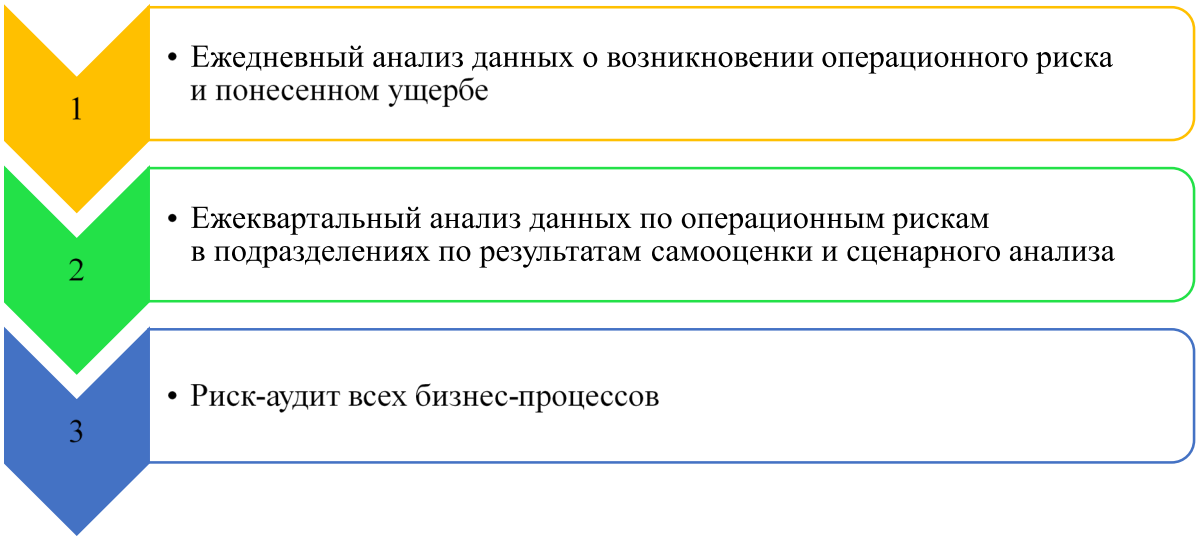

Рисунок 4
Комплекс мер по идентификации операционных рисков

лежности, подвергаются кибератакам. Следовательно, разработка методов защиты от кибератак и реагирования на инциденты является актуальной и обязательной для всех организаций.

Процесс реагирования на инциденты и их обработку может быть представлен следующими основными этапами (рисунок 5).

Под инцидентом будем понимать событие или их комбинацию, указывающие на свер-

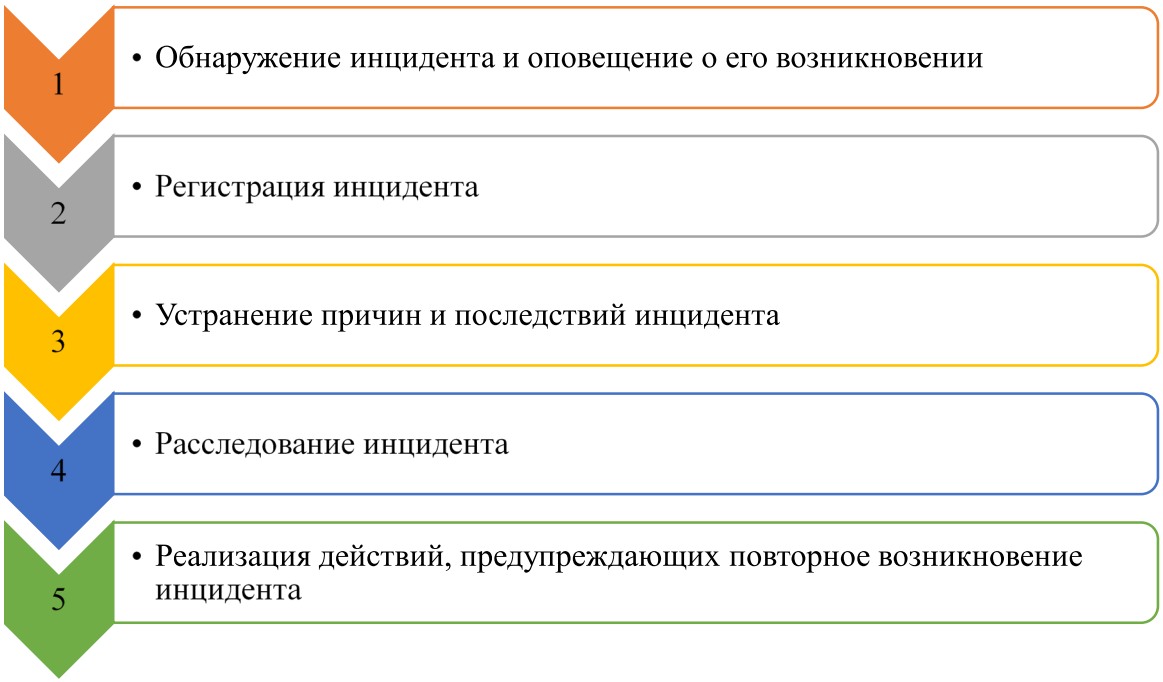

Рисунок 5
Основные этапы реагирования на инцидент ИБ [7]

шившуюся, предпринимаемую или вероятную реализацию угрозы ИБ, результатом которой являются [8]:

- нарушение в системе обеспечения ИБ организации, включая нарушение работы средств защиты информации;
- нарушение требований законодательства Российской Федерации, нормативных актов и предписаний регулирующих и надзорных органов, внутренних документов организации в области обеспечения ИБ, нарушение в выполнении процессов системы менеджмента ИБ организации;
- нарушение в выполнении технологических процессов организации;
- нанесение ущерба как организации, так и ее клиентам [8].

Для своевременного и успешного реагирования на инциденты и их обработку в организации прелагается разработать и внедрить специальную систему оповещения об инцидентах. Состав команды оповещения и способ оповещения следует выбирать в зависимости от особенностей функционирования и структуры организации [9]. Необходимо создать и собственную группу реагирования на инциденты или обращения к внешнему центру реагирования типа CERT, а также разработать инструкции по действиям в условиях инцидентов.

Здесь могут помочь международные стандарты 27035, 27037 (он же ГОСТ), а также рекомендации компаний – признанных специалистов в области расследований (методики Group-IB и Касперского).

В рамках алгоритма обработки инцидента [10], учитывая рекомендации [11; 12], автор предлагает следующую схему реагирования на инцидент ИБ с участием специалистов правоохранительных органов (рисунок 6).

При подготовке данных для расследования инцидентов информационной безопасности источниками данных по инцидентам могут служить:

- лог-серверы – сетевые устройства, серверы, персональные компьютеры (ПК), датчики движения и др.;
- внутренние журналы операционной системы (ОС) устройств (ПК, серверы, сетевые устройства);

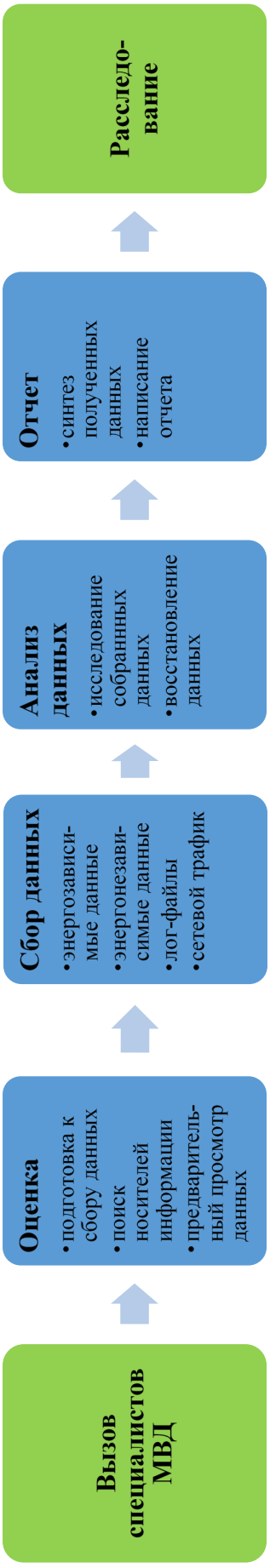

Рисунок 6
Процесс реагирования на инцидент информационной безопасности с привлечением специалистов из МВД

- записи журнала интернет-провайдерам (логи);
- оперативная память (перечень запущенных процессов, сведения о сетевых соединениях, пароли, расшифрованные файлы, ключи шифрования, буфер обмена, зловредный код и т. д.).

Автором рекомендуется на этапе сбора данных следующий набор ПО для расследования инцидентов:

- AccessData FTK Imager – ПО для создания дампа оперативной памяти;
- Volatility Framework – фреймворк для исследования образов содержимого оперативной памяти;
- Digital Forensics Framework – ПО, предназначенное для исследования жестких дисков, энергозависимой памяти и создания отчетов о пользовательских и системных действиях;
- EventLogExplorer – ПО для просмотра системной активности;
- MiTec Windows Registry Recovery – ПО, которое позволяет просматривать изменения реестра;
- MozillaCacheView и подобное ПО для просмотра браузерной активности;
- Internet Evidence Finder Portable – ПО для поиска артефактов интернет-активности на ПК;
- Belkasoft – ПО для произведения компьютерно-технических экспертиз, компьютерной криминалистики, поиска, анализа и хранения цифровых улик (форензики).

На этапе анализа данных изучаются следующие факты:

- названия файлов;
- временные метки;
- нетипичное расположение;
- расширения файлов;
- цифровой слепок файла (хэш).

Этап составления отчета представляет собой процесс подготовки и представления информации, полученной на предыдущих этапах. При формировании отчета следует обратить внимание на следующее [10].

1. Целевая аудитория, которая будет ознакомлена с отчетом. Например, для инцидента, требующего участия правоохранительных органов, потребуется подробный отчет обо всех собранных данных, и скорее всего, копии всех данных, которые могут служить доказательствами. Системного администратора прежде всего заинтересует сетевой трафик и связанная с ним статистика и т. п.

2. Собранные доказательства форензики, альтернативные объяснения. Если информация об инциденте является неполной, тогда невозможно однозначно определить, что произошло. Поэтому если событие имеет несколько правдоподобных объяснений, то в отчете необходимо предоставить доказательства или опровержения каждого возможного объяснения.

3. Основные моменты инцидента, актуальная информация. В отчёт также следует включить полезную информацию, которая может быть использована для предотвращения возможных будущих инцидентов (например, обнаруженные в ходе анализа данных вредоносное ПО или уязвимость). Поэтому все собранные в ходе расследования доказательства должны быть защищены, так как они могут содержать информацию об уязвимостях информационной системы организации.

4. Выводы, меры по предотвращению новых инцидентов.

В результате проведенного расследования инцидента можно установить следующие факты:

- хронология инцидента;
- IP-адреса, доменные имена ресурсов нарушителей;
- сведения о личности и деятельности нарушителя;
- установление причастности сотрудников организации к инциденту;
- новые вирусы;
- новые способы мошенничества и т. д.

Таким образом, расследование инцидентов позволяет определить «слабые места» в системе защиты информации организации, а значит, принять меры по ее совершенствованию и устранению уязвимостей. В том аспекте экономический эффект может быть подсчитан при помощи методики ROSI (Return On Security Investment, рентабельность инвестиций в обеспечение безопасности) [13].

Наряду со строгими правилами проведения мониторинга и хранения журналов событий, разработка новых методов реагирования на инциденты ИБ, несомненно, повысит эффективность расследования инцидентов, как следствие, снизит возможные финансовые потери, предотвратит потерю репутации организации и кражу данных нарушителями ИБ.

При этом, благодаря изучению накопленного опыта в результате расследования каждого инцидента, снижается риск наступления повторного инцидента и совершенствуется система защиты от целевых кибератак.

Для удержания конкурентных преимуществ организациям, как субъектам хозяйственной деятельности, необходимо защищаться и эффективно реагировать на инциденты.

В большинстве случаев, обеспечив качественное и эффективное реагирование и управление инцидентами ИБ, организация может не только снизить риски, но и предотвратить материальный ущерб.

Список литературы

1. Cybersecurity Ventures. URL: https://cybersecurityventures.com/ (дата обращения: 25.01.2020).
2. Потери организаций от киберпреступности. URL: http://www.tadviser.ru/ (дата обращения: 25.01.2020).
3. *Алексеевских А.* ЦБ передумал закрывать глаза на мелкие кибератаки. URL: https://www.banki.ru/news/bankpress/?id=10065699. (дата обращения: 25.01.2020).
4. Global Emergency Response Team (GERT). URL: www.gertconcept.com (дата обращения: 25.01.2020).
5. *Мареичев П., Шаабан А.* Реагирование на компьютерные инциденты в 2018 году. URL: https://securelist.ru/incident-response-analytics-report-2018/94601/ . (дата обращения: 25.01.2020).
6. Сбербанк. Годовой отчет 2018. URL: https://www.sberbank.com/common/img/uploaded/redirected/com/gosa2019/docs/sberbank-annual_report_2018_rus.pdf (дата обращения: 10.02.2020).
7. Computer Security Incident Handling Guide (NIST.SP.800-61r2) URL: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final. (дата обращения: 25.01.2020).
8. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности» РС БР ИББС-2.5-2014. URL: https://cbr.ru/Content/Document/File/46928/rs-25-14.pdf (дата обращения: 25.01.2020).
9. BS ISO/IEC 27000. Система менеджмента информационной безопасности. URL: http://docs.cntd.ru/document/1200102762 (дата обращения: 25.01.2020).
10. *Майорова Е. В., Черток А. В.* Использование методов форензики при расследовании инцидентов компьютерной безопасности // Технико-технологические проблемы сервиса: научно-технический журнал. СПб.: Изд-во СПбГЭУ, 2019. № 4 (50). С. 36–41.
11. *Васильева И. Н.* Расследование инцидентов информационной безопасности: учебное пособие. СПб.: Изд-во СПбГЭУ, 2019. 113 с.
12. Guide to Integrating Forensic Techniques into Incident Response (NIST.SP. 800-86). URL: https://csrc.nist.gov/ (дата обращения: 25.01.2020).
13. *Васильева И. Н.* Управление рисками информационной безопасности: учебное пособие. СПб.: Изд-во СПбГЭУ, 2016. 177 с.