10. Подковырова Ю.С. Сокращенная форма дознания - пределы доказывания // Законность. — 2018. — № 3. —С. 57 - 59.
11. Стремоухов А.В., Иванов И.А. Использование результатов оперативно-розыскной деятельности в уголовном судопроизводстве: проблемы и пути их решения // Ленинградский юридический журнал. — 2016. — № 1. — С. 185 - 192.
12. Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 18.12.2001 № 174-ФЗ (ред. от 19.02.2018) // СЗ РФ. – 2001. – № 52 (ч. I). – Ст. 4921.
13. Чечетин А.Е Современная оперативно-розыскная деятельность и принуждение // Оперативник (сыщик). — 2015. — № 1. — С. 37-42.
14. Чечетин, А.Е. Основы оперативно-розыскной деятельности: учебное пособие. —5-е изд., доп. и перераб. / Под ред. А.Е. Чечетина, — Барнаул: Барнаул. Юридический институт МВД России, 2017. — С.11.
15. Халиков, А. Н. Оперативно-розыскная деятельность / А. Н. Халиков — РИОР: ИНФРА-М, 2017. — С.73.

МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ИССЛЕДОВАНИЯ ФАКТОРОВ ВЛИЯЮЩИХ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ РАЗЛИЧНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Павенский Юрий Алексеевич
эксперт 5 отдела ЭКЦ ГУ МВД России по Московской области
лейтенант полиции

Косова Любовь Никандровна
доцент кафедры экономики ФГБОУ ВО «Российский государственный университет правосудия» кандидат экономических наук, доцент

Аннотация: *В статье изучены методологические основы исследования факторов влияющих на экономическую безопасность различных объектов информатизации. Разработаны методические рекомендации по противодействию угрозам экономической безопасности, связанные с использованием информационных технологий на объектах информатизации. Сделан вывод о том, что методические рекомендации, основанные на результатах исследования, могут быть полезны организациям, осуществляющим экономическую деятельность, в качестве методики, позволяющей значительно снизить угрозы экономической безопасности.*

Ключевые слова: *экономическая безопасность, объект информатизации, преступления, информационные технологии, методика.*

Abstract: *In the article methodological bases of research of the factors influencing economic safety of different information objects. Developed guidelines to address threats to economic security associated with the use of information technology in the information objects. It is concluded that the methodological recommendations based on the results of the study can be useful for organizations engaged in economic activities as a method to significantly reduce the threat to economic security.*

Key words: *economic security, object of Informatization, crimes, information technologies, method.*

Введение. На сегодняшний день современное общество в своей повседневной деятельности использует различные информационные технологии позволяющие производить различные операции с денежными средствами, получать удаленный доступ к компьютерной технике, осуществлять поиск, сбор и обработку необходимой информации, и многие другие действия.

Банки и финансовые организации являются основными финансовыми посредниками в экономике государства. Продолжается тенденция роста количества целевых атак на банки и финансовые орга-

низации. На сегодняшний день общий объем совершенных хищений достиг более 39,8 млрд. рублей.

Актуальность темы заключается в том, что на сегодняшний день большинство организаций, осуществляющих экономическую деятельность, могут быть подвержены различным преступлениям с использованием информационных технологий.

Сачков Илья, Баулин Валерий и Волков Дмитрий отмечают, что необходимо анализировать технические и организационные методы данных преступлений для их эффективного противодействия[1].

Цель исследования: изучить методологические основы исследования факторов влияющих на экономическую безопасность различных объектов информатизации.

Цель исследования может быть достигнута посредством решения следующих задач:

- рассмотрением современных угроз экономической безопасности в России;
- состоит в разработке методических рекомендаций по противодействию угрозам экономической безопасности, связанной с использованием информационных технологий, на объектах информатизации.

Основополагающими методами исследования факторов влияющих на экономическую безопасность являются:

1. анализ и синтез;
2. индукция и дедукция;
3. формализация и моделирование возможных угроз информационной безопасности на объектах информатизации.

Выявлены следующие факторы:

1. угрозы, связанные с работой автоматизированных систем;
2. угрозы, связанные с человеческим фактором.

Разработаны методические рекомендации по противодействию угрозам экономической безопасности, связанной с использованием информационных технологий, на объектах информатизации

Методические рекомендации по противодействию угрозам экономической безопасности, связанной с использованием информационных технологий, на объектах информатизации

Рассмотрим, в чем состоит техника противодействия угрозам экономической безопасности, связанной с использованием информационных технологий.

1. Обеспечение безопасности пользовательских учетных данных организации. Все сотрудники должны быть проинструктированы о том, что все электронные идентификаторы и данные для аутентификации и идентификации нельзя использовать в сторонних от работы целях, передавать их без разрешения руководителя, его заместителей (начальников отделов) другим сотрудникам компании или третьим лицам.

2. Организация мероприятий направленных на обучение и поддержание знаний сотрудников организации по информационной безопасности. Проведение таких мероприятий позволит сотрудникам организации иметь актуальные данные о существующих методах социальной инженерии, а также постоянно помнить про основные правила обеспечения информационной безопасности объекта информатизации.

3. Обеспечение сотрудников организации регламентом по безопасности. Например, в регламенте можно указать, какие необходимо предпринять действия при попытке третьего лица запросить закрытую информацию (например, учетные данные сотрудников).

4. Обеспечение безопасности персональных компьютеров сотрудников организации программными, аппаратными и программно-аппаратными комплексами.

1. Система защиты информации от несанкционированного доступа должна обеспечивать персональный компьютер сотрудника:

- от доступа к информации в нарушение должностных полномочий сотрудников;
- от доступа к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения;
- от доступа к информации в объеме, превышающем необходимый для выполнения служебных обязанностей.

В качестве примера таких комплексов, можно отнести:

- программно-аппаратный комплекс «Соболь»;
- программный комплекс «Secret Net»;
- программный комплекс «Dallas Lock» и т.д.

2. Установленная система защиты информации от несанкционированного доступа должна позволять в качестве средства опознавания пользователей системы использовать электронные идентификаторы:

- USB-Flash-накопители;
- электронные ключи Touch Memory (iButton);
- USB-ключи Aladdin eToken Pro/Java;
- смарт-карты Aladdin eToken Pro/SC;
- USB-ключи Rutoken (Рутокен) и Rutoken ЭЦП.

3. Необходимо произвести настройку учетных записей установленной операционной системы, а именно для доступа к данным нужно использовать не менее двух локальных учетных записей - «администратор» и «пользователь».

4. Необходимо произвести некоторые настройки BIOS:

- отключить загрузку с внешних устройств;
- установите пароль в BIOS.

5. Необходимо установить парольную политику для всех учетных записей сотрудников организации.

6. Необходимо настроить межсетевой экран или использовать изолированную сетевую инфраструктуру.

7. Необходимо настроить аудит для всех учетных записей сотрудников организации;

8. Необходимо настроить некоторые ограничения по использованию учетных записей сотрудниками организации;

9. Необходимо поставить сертифицированное антивирусное программное обеспечение.

5. Все сотрудники должны четко понимать, как вести себя с посетителями. Посетителей всегда должен сопровождать кто-то из сотрудников организации. Если сотрудник встречает неизвестного ему посетителя, он должен в корректной форме поинтересоваться, с какой целью посетитель находится в данном помещении и где его сопровождение. При необходимости сотрудник должен сообщить о неизвестном посетителе в службу безопасности.

Заключение

С помощью различных методов были исследованы факторы и их влияние на экономическую безопасность с использованием информационных технологий различных объектов информатизации осуществляющих экономическую деятельность. Используя различные методы противодействия угрозам экономической безопасности можно снизить уровень ущерба от злоумышленников.

Методические рекомендации, основанные на результатах исследования, могут быть полезны организациям, осуществляющим экономическую деятельность, в качестве методики, позволяющей значительно снизить угрозы экономической безопасности.

Список литературы

1. Воронин А.С. Мошенничество в платежной сфере: Бизнес-энциклопедия. М.: «Центр исследований платежных систем и расчетов. Интеллектуальная Литература», 2016. С. 7.

ВЕРОЯТНОСТНЫЙ АНАЛИЗ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Бритвина Валентина Валентиновна
Кандидат педагогических наук, доцент кафедры «Математика»
Московский политехнический университет

Аннотация: *В статье проанализировали вероятностный анализ безопасности в информационных системах. Определили его значимость при обеспечении ИБ в ИС.*

Ключевые слова: *Вероятностный анализ, информационная безопасность, информационные системы, Значимость.*

Abstract: *The article analyzes the probabilistic analysis of security in information systems. Determined its importance in ensuring the IB in IP.*

Keywords: *Probabilistic analysis, information security, information systems, Significance.*

Введение. Безопасность информации в информационных системах является очень важным вопросом. Так как, информация, находящаяся на электронных носителях играет большую роль в жизни современного общества. На сегодняшний день проблемам информационной безопасности (ИБ) как в масштабах государства, так и в масштабах отдельного предприятия уделяется достаточное внимание, несмотря на это, количество потенциальных угроз не становится меньше [1]

Цели исследования: Выявить необходимость вероятностного анализа безопасности в информационных системах.

Задачи исследования:

1. Определить сферы и значимость использования вероятностного анализа в сфере ИБ

Результат исследования

В качестве основного показателя в вероятностных моделях обнаружения компьютерных атак используется:

– вероятность появления новой формы пакета передачи данных отличной от эталонной;

– математическое ожидание и дисперсия случайных величин, характеризующих изменение IP-адресов источника и потребителя информации, номеров портов АРМ источников и потребителей информации.

Статистические методы дают хорошие результаты на малом подмножестве компьютерных атак из всего множества возможных атак. Недостаток статистических моделей обнаружения аномальных отклонений состоит в том, что они не позволяют оценить объем передаваемых данных и не способны обнаружить вторжения атак с искаженными данными. Узким местом методов является возможность переполнения буфера пороговых проверок «спамом» ложных сообщений.

Для эффективного использования статистических моделей в методе обнаружения аномальных отклонений необходимы строго заданные решающие правила и проверка ключевых слов (порогов срабатывания) на различных уровнях протоколов переда-