УДК 378
DOI 10.33764/2618-981X-2022-6-311-317

Политика информационной безопасности в организации

А. М. Язовский[1], А. В. Шабурова[1], Н. Л. Гавриленко[1]*
[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: yazovski_alexander@mail.ru

Аннотация. В данной статье рассматривается проблема по обеспечению информационной безопасности многих организаций, связанная с разработанными и действующими политиками информационной безопасности в этих организациях. Актуальность работы обусловлена наличием пробелов, уязвимостей и изъянов в обеспечении безопасности информации организации STS Logistics, в связи с чем увеличивается риск несанкционированного доступа к информационным ресурсам компании и раскрытию персональных данных сотрудников. Цель работы заключается в выявлении недостатков в обеспечении безопасности информации в рассматриваемой организации со стороны существующей политики информационной безопасности, путем разработки модели угроз и анализа действующей политики информационной безопасности. На основании проделанной работы необходимо выявить угрозы, создающие предпосылки для возможной утечки защищаемой информации и разработать рекомендации по совершенствованию политики информационной безопасности для их ликвидации. Проводимое исследование заключается в построении модели угроз безопасности информации и в анализе политики информационной безопасности, существующей в данной организации.

Ключевые слова: политика информационной безопасности, информационная безопасность, подготовка специалистов

Information security policy in the organization

A. M. Yazovski[1], A. V. Shaburova[1], N. L. Gavrilenko[1]*
[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: yazovski_alexander@mail.ru

Abstract. This article discusses the problem of ensuring the information security of many organizations associated with the developed and current information security policies in these organizations. The relevance of the work is due to the presence of gaps, vulnerabilities and flaws in ensuring the security of information of the STS Logistics organization, which increases the risk of unauthorized access to the company's information resources and the disclosure of personal data of employees. The purpose of the work is to identify shortcomings in ensuring the security of information in the organization under consideration from the existing information security policy, by developing a threat model and analyzing the current information security policy. Based on the work done, identify threats that create prerequisites, the possibility of leakage of protected information and develop recommendations for improving the information security policy to eliminate them. The ongoing research consists in building a model of information security threats and in analyzing the information security policy that exists in a given organization.

Keywords: information security policy, information security, training of specialists

Введение

В настоящее время информация, в виде отдельного ресурса, имеет ключевую значимость во многих сферах жизни человека, а также является главным ресурсом развития общества [1]. В настоящее время в мире компьютерных технологий продолжает возрастать количество киберпреступлений. Вместе с этим, насущной проблемой становится не только поиск несовершенств в системе подготовки специалистов в области информационной безопасности (далее – ИБ), но и пересмотр, формирование действующей Политики информационной безопасности в организациях.

Политикой ИБ называется комплекс мер, правил и принципов, которыми руководствуются сотрудники организаций для защиты информации.

В наше время сформировано большое количество политик – в каждой конкретной организации руководство определяет, как и каким образом защищать информационные ресурсы организации, но проработанность данных политик не всегда соответствует качественному уровню защиты ресурсов этих организаций [4].

Основным методом для решения проблемы обеспечения безопасности информации различного рода организаций является более детальная проработка, анализ и предложения по совершенствованию, с учетом имеющихся недостатков, действующих политик информационной безопасности этих организаций, для чего необходимо строить модель угроз, которая укажет на слабые места осуществления защиты информационных ресурсов.

Поэтому цель данной статьи заключается в выявлении недостатков процесса обеспечения безопасности информации в рассматриваемой организации STS Logistics путем разработки модели угроз и анализа действующей политики информационной безопасности. На основании проделанной работы необходимо выявить угрозы, создающие предпосылки для возможной утечки защищаемой информации и разработать рекомендации по совершенствованию политики информационной безопасности для их ликвидации.

Материалы

Политика ИБ – это систематизированное описание высокоуровневых целей и задач защиты, которыми необходимо руководствоваться в своей деятельности.

Обеспечение ИБ – важный элемент для успешного осуществления уставной деятельности организации. Обеспечение ИБ состоит из любой деятельности, направленной на защиту информационных ресурсов. Политика охватывает все автоматизированные и телекоммуникационные системы, владельцем и пользователем которых является организация.

Ответственность за выполнение политики несут все пользователи информационных систем организации. Ответственность сотрудников за несоблюдение требований, которые влекут за собой разглашение или утечку информации ограниченного доступа, определяется законодательством РФ, внутренними нормативными документами предприятия [2].

Реализация политики должна исходить из предпосылки, что невозможно обеспечить требуемый уровень защищённости информационных ресурсов не только с помощью отдельного средства, но и с помощью их совокупности. Необ-

ходимо их системное применение, а отдельные разрабатываемые элементы должны рассматриваться как часть единой информационной системы в защищённом исполнении при оптимальном соотношении технических и организационных мероприятий.

Главной целью, на осуществление которой направлены все положения политики организации, является защита информационных ресурсов от возможного нанесения им негативных последствий, в результате воздействия на информацию, её носители, процессы обработки и передачи [4].

Для достижения данной цели требуется обеспечивать решение следующих задач:

– быстрое выявление, оценка и прогнозирование источников угроз ИБ;
– создание механизма оперативного реагирования на угрозы ИБ;
– предотвращение ущерба от реализации угроз ИБ;
– обеспечение непрерывности критических бизнес-процессов;
– достижение адекватности мер по защите от угроз ИБ;
– изучение партнёров, клиентов, конкурентов и кандидатов на работу;
– недопущение проникновения структур организованной преступности;
– выявление негативной деятельности сотрудников.

Политика ИБ организации выделяет основные разделы:

1. общие положения;
1.1 . цель и назначение;
1.2 . область применения;
2. рекомендации и требования;
2.1 . обязанность за информационные активы;
2.2 . доступ к информационным системам;
2.3 . защита оборудования;
2.4 . определенные регламенты использования электронной почты;
2.5 информация и оповещения об инцидентах ИБ;
2.6 помещения с техническими средствами;
2.7 управление сетью;
2.8 разработка систем и управление внесением изменений [10].

Контроль за выполнением требований политики ИБ производится руководителем подразделения ИБ путем проведения регулярных контрольных мероприятий [5].

Модель угроз ИБ организации STS Logistics

Для того, чтобы выявить имеющиеся слабые места в осуществлении ИБ организации (https://stslog.com), строится модель угроз.

Модель угроз (безопасности информации) – описательное представление свойств или характеристик угроз ИБ.

Определение угроз безопасности информации необходимо для выявления возможности нарушения свойств информации (конфиденциальности, доступности и целостности), содержащихся в информационной системе организации. Нарушение хотя бы одного свойства безопасности информации может привести к негативным последствиям для обладателя информации [3].

На примере организации STS Logistics, в соответствии с методикой оценки угроз информационной безопасности утвержденной ФСТЭК России 05.02.2021 и в соответствии с банком данных угроз ФСТЭК, были определены объекты воздействия нарушителей, интерфейсы, способы реализации угроз, а также построена модель угроз (таблица 1, таблица 2).

Таблица 1

Определение нарушителей, объектов их воздействия и способовреализации угроз безопасности организации STS Logistics

Виды нарушителя	Категории нарушителя	Объект воздействия	Интерфейсы	Способы реализации
Бывшие работники/ конкуренты	Внешний	Автоматизированное рабочее место (далее – АРМ) пользователя: несанкционированный доступ к операционной системе АРМ пользователя; нарушение конфиденциальности информации, содержащейся на АРМ пользователя	Сетевые интерфейсы коммутатора сети	Внедрение вредоносного программного обеспечения
Технический персонал	Внутренний	АРМ пользователя: несанкционированный доступ к операционной системе АРМ пользователя; нарушение конфиденциальности информации, содержащейся на АРМ пользователя	Съемные машинные носители информации, подключенные АРМ пользователя	Использование уязвимостей конфигурации системы управления доступом

Таблица 2

Перечень актуальных угроз безопасности организации STS Logistics

Угроза безопасности информации	Описание угрозы	Источники угрозы	Объект воздействия	Угроза безопасности информации
УБИ 007: Угроза воздействия на программы с высокими привилегиями	Угроза заключается в возможности повышения нарушителем своих привилегий в дискредитированной системе путем использования ошибок в программах и выполнения произвольного кода их привилегиями Данная угроза обусловлена слабостями механизма проверки входных данных и команд, а также мер по ограничению доступа	Внешний/ внутренний нарушитель	Информационная система, виртуальная машина, сетевое программное обеспечение, сетевой трафик	Нарушение конфиденциальности и целостности

Окончание табл. 2

Угроза безопасности информации	Описание угрозы	Источники угрозы	Объект воздействия	Угроза безопасности информации
	Реализация этой угрозы возможна при условиях обладаемой дискредитируемой программой повышенными привилегиями в системе и осуществления дискредитируемой программой приема входных данных от других программ или от пользователя			
Угроза безопасности информации	Описание угрозы	Источники угрозы	Объект воздействия	Последствия реализации угрозы
УБИ 008: Угроза восстановления и/или повторного использования аутентификационной информации	Угроза определяется в возможности доступа к данным пользователя в результате подбора (например, путем полного перебора или перебора по словарю) аутентификационной информации дискредитируемой учетной записи пользователя в системе Данная угроза обусловлена несовершенствами, связанными со значительно меньшим объемом данных хеш-кода аутентификационной информации по сравнению с ней самой	Внутренний/внешний нарушитель	Системное программное обеспечение, микропрограммное обеспечение, учетные данные пользователя	Нарушение конфиденциальности
Угроза безопасности информации	Описание угрозы	Источники угрозы	Объект воздействия	Последствия реализации угрозы
УБИ 037: Угроза исследования приложения через отчеты об ошибках	Угроза заключается в возможности исследования нарушителем алгоритма работы дискредитируемого приложения и его структуры путем анализа генерируемых этим приложением отчетов об ошибках Данная угроза обусловлена размещением защищаемой информации (или информации, обобщение которой может раскрыть защищаемые сведения о системе) в генерируемых отчетах об ошибках Реализация данной угрозы возможна в случае наличия у нарушителя доступа к отчетам об ошибках, генерируемых приложением, и наличия избыточности содержащихся в них данных	Внутренний/ внешний нарушитель	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение	Нарушение конфиденциальности

Таким образом, видно, что для предполагаемого нарушителя объектом воздействия чаще является доступ к операционной системе АРМ пользователя, а также нарушение конфиденциальности информации, находящейся на АРМ пользователя. Способами реализаций данных воздействий могут служить использование уязвимостей конфигурации системы управления доступом и внедрение вредоносного ПО [7].

Результаты

Благодаря построенной модели угроз организации STS Logistics, были выявлены имеющиеся угрозы безопасности информации. Реализация данных угроз может нести следующие негативные последствия:

– нарушение неприкосновенности частной жизни;

– нарушение тайны переписки, разговоров по телефону, планов, иной информации;

– нарушение конфиденциальности (утечка) персональных данных;

– разглашение персональных данных пользователей [8].

Во избежание подобных угроз разработаны рекомендации для совершенствования политики ИБ. Актуальная политика ИБ в рассматриваемой организации должна быть пересмотрена с учетом следующих рекомендаций:

– необходимо постоянное журналирование действий персонала, осуществляющего обслуживание и модификацию программных и технических средств информационной системы;

– требуется подготовка должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации и процессов ее обработки;

– необходим контроль за соблюдением всеми пользователями информационной системы требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

– должна быть персональная ответственность за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам;

– требуется постоянное поддержание необходимого уровня защищенности элементов информационной среды.

Заключение

В данной статье была рассмотрена проблема по осуществлению безопасности информации организации STS Logistics, связанная с действующей политикой ИБ, которая, как показала построенная модель угроз, оказалась несовершенна.

В настоящее время, на основе проведенного исследования, во избежание угроз безопасности информации рассматриваемой организации, разработаны рекомендации по совершенствованию существующей политики ИБ и принято решение по осуществлению пересмотра данной политики ИБ один раз в 3 года с приведением в соответствие определенных политикой защитных мер реальным условиям и текущим требованиям к защите информации.

Внеплановое внесение изменений в политику ИБ может производиться по результатам анализа инцидентов, актуальности, достаточности и эффективности используемых мер обеспечения ИБ, результатам проведения внутренних аудитов ИБ и других контрольных мероприятий [6].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Оюн Ч.О. Основные подходы к формированию политики безопасности /Е. В. Попантонопуло // Интерэкспо Гео-Сибирь. – 2019. – Т. 6. – № 2. – С. 3-7.
2. Грибунин В. Г. Комплексная система защиты информации на предприятии [Текст] : учеб. пособие для студентов высш. учеб. заведений / В. Г. Грибунин, В. В. Чудовский. - М.: Академия, 2009. – 416 с. С 36-41.
3. Наскидашвили К. А. Информационная безопасность. Виды угроз информационной безопасности // Вестник студенческого научного общества ГОУ ВПО "Донецкий национальный университет". – 2020. – Т. 1. – № 12. – С. 187-189.
4. Бржезинская А. Д. Создание политики информационной безопасности и ее влияния на процесс управления безопасностью // Молодежный научный форум: общественные и экономические науки. – 2016. – № 11 (40). – С. 231-235.
5. Шевченко А.В. Управление безопасностью информационных процессов / А.В. Шевченко. – М. : РАГС, 2009. – 138 с.
6. Бондаренко Н. А. О корпоративной политике информационной безопасности предприятия /А. Д. Буханцов, П. Г. Лихолоб, А. В. Помельников // В сборнике: Актуальные вопросы обеспечения информационной безопасности. Белгородский университет кооперации, экономики и права. – 2015. – С. 85-92.
7. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты : учеб. пособие / А. Ю. Щербаков – М. : Кн. мир, 2009. – 352 с.
8. Шевченко А. В. Управление безопасностью информационных процессов : учеб. пособие / А. В. Шевченко. – М. : РАГС, 2009. – 138 с.
9. Быстряков Е. В. Формирование политики информационной безопасности в организации: стратегические задачи и их реализация / С. А. Быстрякова // В сборнике: Бачиловские чтения. Материалы четвертой международной научно-практической конференции. отв. ред. Т.А. Полякова, А. В. Минбалеев, В. Б. Наумов / Институт государства и права РАН. Саратов. – 2022. – С. 396-403.
10. Филиппова Е. А. Концептуальные положения политики информационной безопасности в организации // Научный обозреватель. –2016. – № 6. – С. 63-64.