МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

МАТЕРИАЛЫ
IX Всероссийской научно-практической конференции
с международным участием

г. Волгоград, 27–28 октября 2021 г.

Волгоград 2021

УДК 681.5(042)
ББК 32.81я43
Б40

Безопасность информационных систем и технологий в условиях
Б40 цифровой экономики [Текст] : материалы IX Всерос. науч.-практ. конф. с междунар. участием, г. Волгоград, 27–28 окт. 2021 г. / редкол.: О. А. Какорина, Ю. С. Бахрачева, Т. А. Попова ; Федер. гос. авт. образоват. учреждение высш. образования «Волгогр. гос. ун-т». – Волгоград : Изд-во ВолГУ, 2021. – 104 с.

ISBN 978-5-9669-2166-8

Настоящий сборник составлен по материалам IX Всероссийской научно-практической конференции с международным участием «Безопасность информационных систем и технологий в условиях цифровой экономики», проведенной 27–28 октября 2021 г. в Волгоградском государственном университете. В состав оргкомитета конференции вошли ведущие российские и зарубежные ученые, а также известные специалисты в области информационной безопасности. В сборнике научных трудов представлены избранные доклады и тезисы статей, в которых рассматриваются современные проблемы в области информационной безопасности.

Сборник предназначен для профильных специалистов, научных работников, преподавателей, аспирантов, магистрантов, студентов с целью использования в научной работе и учебной деятельности.

УДК 681.5(042)
ББК 32.81я43

ISBN 978-5-9669-2166-8

Астафурова Ольга Анатольевна
кандидат технических наук, заведующая кафедрой
информационных систем и математического моделирования ВИУ РАНХиГС
astoa@vlgr.ranepa.ru
Омельченко Татьяна Александровна
старший преподаватель кафедры информационной безопасности
Волгоградского государственного университета
omelchenko.tatiana@volsu.ru
Голоманчук Эйда Владимировна
кандидат юридических наук, доцент кафедры
конституционного и административного права ВИУ РАНХиГС
golomanchukav@mail.ru

РАЗРАБОТКА ПРОГРАММНОГО СРЕДСТВА ОЦЕНКИ ЗНАНИЙ ГОСУДАРСТВЕННЫХ СЛУЖАЩИХ ПО ВОПРОСАМ ПРОТИВОДЕЙСТВИЯ КОРРУПЦИИ [1]

Аннотация. В статье рассмотрены вопросы разработки программного средства оценки знаний государственных служащих по вопросам противодействия коррупции. Представлена и описана архитектура программы, системные требования и основные возможности.

Ключевые слова: информационные технологии, информационно-аналитическая система, оценка знаний по вопросам противодействия коррупции, профилактика и противодействие коррупционным процессам.

DEVELOPMENT OF A SOFTWARE FOR ASSESSING THE KNOWLEDGE OF CIVIL SERVANTS ON ANTI-CORRUPTION ISSUES [1]

Astafurova Olga Anatolyevna
Candidate of Technical Sciences, Head of the Department
of Information Systems and Mathematical Modeling of the VIU RANEPA
astoa@vlgr.ranepa.ru

Omelchenko Tatiana Alexandrovna
Senior Lecturer of the Department of Information Security
of Volgograd State University
omelchenko.tatiana@volsu.ru
Golomanchuk Eida Vladimirovna
Candidate of Legal Sciences, Associate Professor
of the Department of Constitutional and Administrative Law of the VIU RANEPA
golomanchukav@mail.ru

Abstract. The article discusses the issues of developing a software tool for assessing the knowledge of civil servants on anti-corruption issues. The program architecture, system requirements and main features are presented and described.

Key words: information technologies, information and analytical system, assessment of knowledge on anti-corruption issues, prevention and counteraction to corruption processes.

На сегодняшний день наиболее актуальной проблемой, препятствующей стабильному развитию и эффективному функционированию государственных органов, различных систем и сфер деятельности являются коррупционные процессы. Для их профилактики необходимо на постоянной основе проводить тематические семинары, лекции и тестирования, направленные на повышение общего уровня юридической грамотности и правового просвещения государственных гражданских служащих [1].

Применение современных информационных технологий при проведении профилактических работ в вопросах противодействия коррупции позволяет в значительной степени упростить деятельность по информированию граждан, автоматизировать работы, связанные с проведением тестирований, сбором и обработкой аналитической информации [2, 4]. Логическим развитием идеи применения информационных технологий для организации процесса приобретения знаний и навыков по

противодействию коррупции является разработка программного средства оценки знаний государственных служащих по вопросам противодействия коррупции в рамках гранта РФФИ «Формирование антикоррупционной среды в органе государственной и муниципальной власти путем внедрения информационно-аналитической системы «Методика и тактика противодействия коррупции для государственных и муниципальных служащих» [3, 5].

Разработанное программное средство представляет собой один из модулей, подключаемых к информационно-аналитической системе, и выполняет функции авторизации пользователя, выбора теста из списка тестов доступных для прохождения, опроса пользователя по выбранному тесту с сохранением результатов в базе данных для дальнейшего анализа, а также ограниченный в данной версии программы функционал учетной записи аналитика [1].

Архитектура тестовой системы оценки знаний государственных служащих по вопросам противодействия коррупции приведена на рисунке 1.

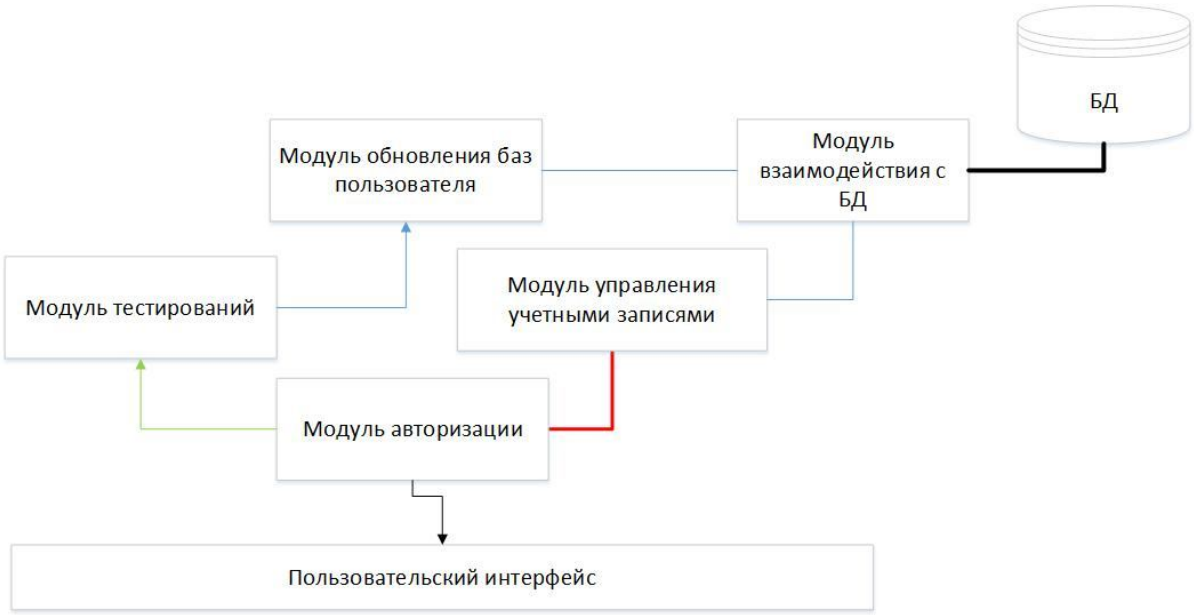

Рис. 1. Архитектура программного средства оценки знаний государственных служащих по вопросам противодействия коррупции

Модуль авторизации предназначен для регистрации учетных записей пользователей программного средства. При первом входе в систему

указанный логин и пароль сохраняется в качестве новой учетной записи в специально отведенной для этого таблице базы данных. При каждом последующем входе в тестовую систему, с использованием сохраненного логина, в базу данных тестирований будет добавляться и обновляться информация о пройденных тестах под этой учетной записью.

Модуль управления учетными записями доступен только для встроенной в программное средство системной записи аналитика. Он позволяет ознакомится с информацией обо всех зарегистрированных в процессе эксплуатации тестовой системы учетных записях и результатах тестирований. Авторизация под учетной записью аналитика запускает соответствующий интерфейс, отличный от интерфейса взаимодействия с остальными пользователями.

Модуль тестирований представлен четырьмя тестирующими оболочками с областью вывода текущего вопроса, областью с выводом вариантов ответа на текущий вопрос, счетчиком времени и кнопкой подтверждения выбора ответа. На выполнение каждого теста отводится определенный временной интервал, по завершении которого тест закрывается принудительно и текущий результат прохождения сохраняется в соответствующую таблицу базы данных. В процессе тестирования пользователь может отслеживать затраченное время по таймеру.

Модуль обновления баз пользователя взаимодействует с модулем тестирований, позволяя автоматически вносить изменения в базу данных.

Модуль взаимодействия с базой данных является провайдером базы данных и реализует программное управление операциями в базе данных.

База данных содержит в себе информацию о зарегистрированных пользователях системы и результаты тестирований.

Пользовательский интерфейс представляет собой графическую оболочку, осуществляющую взаимодействие пользователя и тестовой системы.

Программный продукт предназначен для использования в операционных системах семейства Windows. Тестирование проводилось для

версий Windows 7 и Windows10, с использованием средств разработки MS Visual Studio 2019 на языке программирования C#. Основным требованием для корректной работы программного средства оценки знаний государственных служащих по вопросам противодействия коррупции является наличие двух основных компонент: .NetFramework не ниже версии 4.7 для обеспечения работы модулей, и MSSQLlocalDB для обеспечения взаимодействия с базами данных. Указанные компоненты входят в установочный пакет, который проверяет их наличие и соответствие версий перед началом установки программы. Исходя из результатов проверки, в случае отсутствия указанных компонентов или несоответствия версий, будет произведена их загрузка и установка.

Программное средство способно проводить тестирование по четырем методикам: «Программа оценки психологических предпосылок коррупционных действий сотрудников» (тест 1), «Программа оценки сотрудников по вопросам противодействия коррупции» (тест 2), «Программа оценки знаний государственных служащих по вопросам предоставлений сведений о доходах» (тест 3), «Программа оценки девиантных отклонений сотрудников» (тест 4) [6].

Методика теста 1 предполагает оценку ответов согласно семи установленным шкалам, аналогично, методика теста 4 оценивает ответы тестируемых по шести установленным шкалам. Каждая шкала имеет пограничное значение – норму, превышение которой позволяет судить о тех или иных девиациях в поведении. По результатам проведенных тестирований были подсчитаны средние показатели по каждой из шкал тестов, а также показатели максимального отклонения от нормы среди тестируемых.

Методика теста 2 и теста 3 предполагает подсчет количества баллов по числу правильных ответов. Максимальный балл для теста 2 – 20 баллов (20 вопросов), а для теста 3 – 45 баллов (45 вопросов). Предметом тестирований является знание правовых норм в области коррупции.

Внедрение в деятельность подразделений по противодействию коррупционных и иных правонарушений информационно-аналитической системы позволит развить профилактическое направление в предупреждении коррупции и осуществить развитие антикоррупционного образования. Предлагаемый программный продукт позволит автоматизировать оценку знаний государственных служащих по вопросам владения ими основами антикоррупционного законодательства, по предоставлению сведений о доходах, по аналитике психологического состояния, денежного поведения и его предпосылок, по изучению склонности должностных лиц к коррупции.

Примечание

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16119 «Формирование антикоррупционной среды в органе государственной и муниципальной власти путем внедрения информационно-аналитической системы “Методика и тактика противодействия коррупции для государственных и муниципальных служащих”»

Список литературы

1. Use of modern information technologies for countering corruption in the executive authorities / O. A. Astafurova, A. S. Borisova, E. V. Golomanchuk, T. Y. Yagotinsteva // International Journal of Information and Education Technology. 2020. Vol. 10. No. 3. Pp. 209–214. DOI: 10.18178/ijiet.2020.10.3.1365.

2. Голоманчук Э. В., Яготинцева Т. Ю., Астафурова О. А. Отдельные проблемы правового регулирования процесса осуществления контроля над расходами должностных лиц в Российской Федерации // Бизнес. Образование. Право. 2021. № 3 (56). С. 243–250. DOI: 10.25683/VOLBI.2021.56.361.

3. Астафурова О. А., Борисова А. С., Омельченко Т. А. Концептуальная модель практико-ориентированной информационно-аналитической системы противодействия коррупции // Бизнес. Образование. Право. 2019. № 3(48). С. 238–243. DOI: 10.25683/VOLBI.2019.48.348.

4. Anti-corruption education of public officers using digital technologies / O. A. Astafurova, A. S. Borisova, E. V. Golomanchuk, T. A. Omelchenko // International Journal of Information and Education Technology. 2020. Vol. 10. No. 2. Pp. 90–94. DOI: 10.18178/ijiet.2020.10.2.1345.

5. Астафурова О. А., Борисова А. С., Омельченко Т. А. Концептуальная модель практико-ориентированной информационно-аналитической системы противодействия коррупции // Бизнес. Образование. Право. 2019. № 3(48). С. 238–243. DOI: 10.25683/VOLBI.2019.48.348.

6. Analysis of knowledge assessment results of civil servants regarding anti-corruption issues / Olga Astafurova, Ada Golomanchuk, Tatyana Omelchenko, Anna Borisova and Julia Kayushnikova / SHS Web Conf. International Scientific and Practical Conference “Law and the Information Society: Digital Approach” (LISID-2020). 2021. Vol. 109. DOI: https://doi.org/10.1051/shsconf/202110901006 // [Электронный ресурс] – Режим доступа: https://www.shs-conferences.org/articles/shsconf/abs/2021/20/shsconf_lisid2021_01006/shsconf_lisid2021_01006.html (Дата обращения: 15.07.2021)

ОПРЕДЕЛЕНИЕ СОСТАВА СИСТЕМЫ ЗАЩИТЫ ПЛАТЕЖНЫХ СИСТЕМ

Бабенко Алексей Александрович
кандидат педагогических наук,
доцент кафедры информационной безопасности
Волгоградского государственного университета
ba_benko@mail.ru
Проспект Университетский, 100, 400062 г. Волгоград, Российская Федерация
Оладько Никита Денисович
студент 4 курса кафедры информационной безопасности
Волгоградского государственного университета
ibas-181_113577@volsu.ru
Проспект Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Рассмотрены разные виды платежных систем. Определены вопросы безопасности использования платежных систем, найдено решение проблемы выбора средств защиты информации для защиты платежных систем.

Ключевые слова: платежные системы, персональные данные, конфиденциальность, целостность, аутентификация, средства платежа, авторизация, транзакция, средство защиты информации.

DETERMINING THE COMPOSITION OF THE PAYMENT SYSTEM PROTECTION SYSTEM

Babenko Alexey Alexandrovich

Volgograd State University, the department of informational security,

PhD, associated professor

ba_benko@mail.ru

100, Universitetsky pr. Volgograd, 400062, Russia

Olad'ko Nikita Denisovich

Volgograd State University, the department of informational security,

4th year student

ibas-181_113577@volsu.ru

100, Universitetsky pr. Volgograd, 400062, Russia

Abstract. Different types of payment systems are considered. The issues of security of using payment systems are identified, a solution to the problem of choosing information security tools for protecting payment systems is found.

Key words: payment systems, personal data, confidentiality, integrity, authentication, means of payment, authorization, transaction, information security tool.

В настоящее время платежные системы из-за повсеместной распространенности представляют повышенную опасность для пользователей. Интернет-покупки содержат важную и конфиденциальную

информацию, начиная от места жительства, если покупка с доставкой, заканчивая информацией платежного средства человека. Очень много людей и компаний каждый день совершают миллионы транзакций через различные платежные системы.

Очень важным вопросом при использовании платежной системы является ее безопасность от внешних и внутренних угроз. Существует множество способов обеспечения безопасности платежной системы. Способы же представляют собой различные методы и имеют совершенно разную эффективность.

В данной области рассматриваются разные подходы к классификации платежных систем.

Рассмотрим виды платежных систем (рисунок 1):

Рис. 1. Разновидности платежных систем

Дебетовые – виды систем, которые обрабатывают электронные деньги и цифровые чеки;

Кредитные – виды систем, работающих с кредитными картами [1, 2].

Перед совершением платежа в данных системах проверяется соответствие следующих условий проведения оплаты:

1. Конфиденциальность. Номер банковской карты и другие личные данные владельца счета при совершении банковских операций при помощи карты или в сети остаются частной информацией, доступ к которой имеет только банк.

2. Целостность. До, после и во время транзакции все данные о продукте и условиях продажи не изменятся.

3. Аутентификация. Лицо, участвующее в транзакции, будет использовать только актуальные данные, которые фактически подтверждены.

4. Средства платежа. Клиент может выбирать способы оплаты заказа и валюты для транзакции.

5. Авторизация. Транзакция совершается только при наличии необходимой суммы свободных средств на счете покупателя.

6. Гарантия рисков продавца и покупателя со стороны поставщиков и других участников цепочки транзакций, например, провайдера.

7. Транзакция. Снижение комиссии за совершение банковских операций увеличивает количество пользователей.

Данная цепочка проверок при недостаточной защищенности системы может привести к перехвату данных злоумышленником.

Согласно результатам исследования, проведенного «Positive Technologies» в 2018 г., 61% исследованных онлайн банков имеет низкий уровень защищенности. Основная проблема низкого уровня защищенности заключается в неправильных настройках средств защиты информации (СрЗИ), ошибок в логике работы банка.

Такие ошибки в работе банка несут не только опасность получения персональных данных (ПДн) клиента, но и нарушение в бизнес-логике системы банка.

Также исследование показывает, что большинство банков используют программное обеспечение (ПО) собственной разработки (рисунок 2).

Использование программных решений от вендоров имеет меньше уязвимостей чем собственное ПО. Из чего и вытекает основная проблема в

виде некорректных настроек, т.к. если вендоры допускают уязвимости на этапе проектирования, то в собственное ПО уязвимости закладываются на этапе кода.

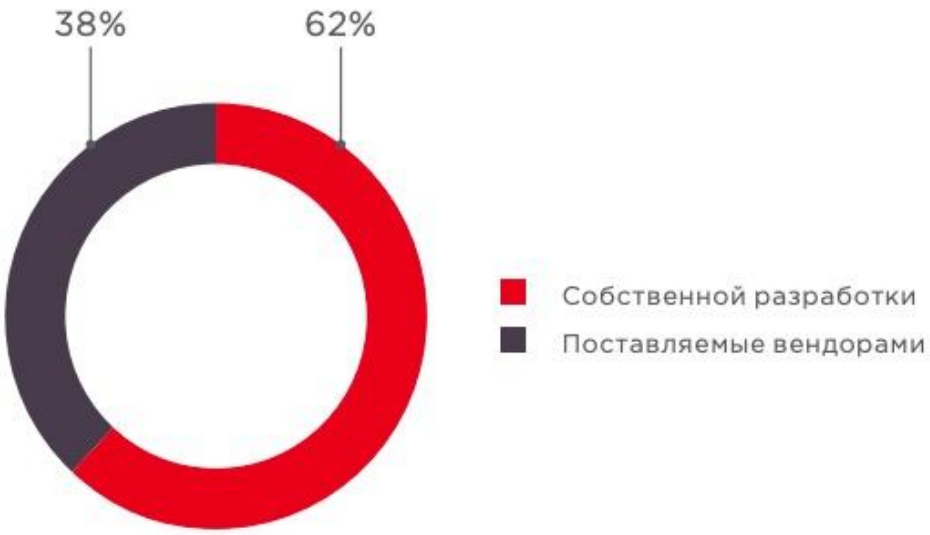

Рис. 2. Сравнение использования ПО банками

Мы предлагаем решение проблемы выбора СрЗИ методом подбора необходимых решений на каждом этапе работы банка. Данный метод реализуется с помощью программы, которая определяет список подходящих СрЗИ в зависимости от требуемых функций. Следовательно, организация которой требуется набор СрЗИ, смогут подобрать решения исходя из текущей ситуации на рынке. Каждому СрЗИ можно присвоить ту или иную оценку по различным требованиям и отследить лучшую, тогда при обновлении требований можно будет изменить оценку средства и подобрать другой набор.

Разработанная программа позволяет экспертным методом определить необходимость того или иного СрЗИ в зависимости от текущих условий в сфере ИБ. Оценка средств происходит по требованиям ФСТЭК, ФСБ, нормативных актов [1,2]. Данный подход позволит увеличить использование удобного и подходящего под определенную ситуацию профессионального ПО и уменьшить критические ошибки в работе платежных систем.

Список литературы

1. Федеральный закон «О национальной платежной системе» от 27.06.2011 № 161-ФЗ.

2. Положение Банка России от 19.06.2012 № 383-П (ред. от 11.10.2018) «О правилах осуществления перевода денежных средств».

3. Анализ уязвимости онлайн-банков [Электронный ресурс] // Positive Technologies. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Vulnerabilities-RBO-2019-rus.pdf.

АНАЛИЗ ПОДХОДОВ К ОБЕСПЕЧЕНИЮ НАДЕЖНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Бандурова Елизавета Евгеньевна

Студент кафедры информационной безопасности

Волгоградского государственного университета

ibb-181_837244@volsu.ru

Проспект Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Рассмотрены основные подходы к обеспечению надежности объектов информационных систем, выделены критерии для их оценки, проведен сравнительный анализ подходов обеспечения надежности объектов информационных систем.

Ключевые слова: надежность, информационная система, предупреждение ошибок, обнаружение ошибок, исправление ошибок, устойчивость к ошибкам.

ANALYSIS OF APPROACHES TO ENSURING THE RELIABILITY OF INFORMATION SYSTEMS

Bandurova Elizaveta Evgen'evna

Student of Department of Information Security,

Volgograd State University

ibb-181_837244@volsu.ru

Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation

Abstract. The main approaches to ensuring the reliability of information system objects are considered, criteria for their evaluation are identified, a comparative analysis of approaches to ensuring the reliability of information system objects is carried out.

Key words: reliability, information system, error prevention, error detection, error correction, error tolerance.

Информационная система (ИС) по определению содержит следующие группы объектов: информацию, базы данных, информационные технологии и технические средства. Каждый объект ИС имеет свои особенности, влияющие на возникновение угроз.

Для того чтобы сопоставить выделенным объектам угрозы, влияющие на надежность необходимо проанализировать факторы, определяющие возникновение угроз на объектах ИС, угрозы безопасности, в том числе описанные в банке данных угроз безопасности информации ФСТЭК России и базовой модели угроз [2] (рисунок 1).

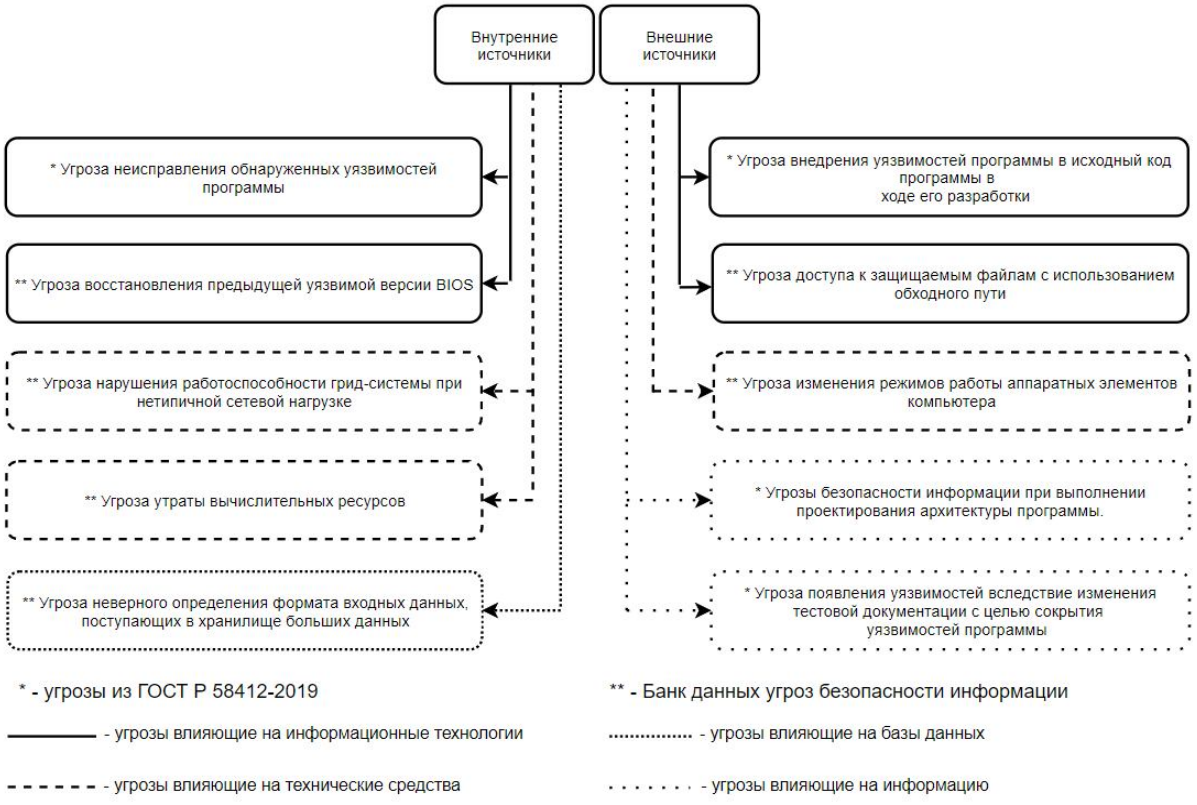

Рис. 1. Угрозы, влияющие на надежность объектов информационной системы

Выделяют четыре основных подхода к обеспечению надежности объектов информационной системы [3, 4]:

1) предупреждение ошибок;
2) обнаружение ошибок;
3) исправление ошибок;
4) обеспечение устойчивости к ошибкам.

Для проведения сравнительного анализа подходов обеспечения надежности объектов информационных систем выделены следующие критерии: возможность восстановления исходного состояния системы; возможность выполнения резервирования; отказоустойчивость; тестирование; сложность реализации; возможность устранения ошибок на этапе проектирования системы и возможность предпринять единые действия для всех компонентов системы при обнаружении ошибок. Соответствие критериев и их качественных характеристик (возможные значений), представлено на рисунке 2.

Рис. 2. Критерии оценки и их возможные значения для анализа подходов обеспечения надежности объектов информационной системы

Качественные характеристики выделенных критериев приведены в соответствие количественным, что позволило проанализировать подходы к обеспечению надежности объектов информационных систем. Сравнение походов проводилось при помощи подсчета расстояния Хемминга.

Подход обеспечения устойчивости к ошибкам получил наименьшую результирующую, и следовательно, наилучшую оценку по результатам сравнения всех подходов по всем критериям. Тем не менее, он является сложно реализуемым. Поэтому принято решение более подробно рассмотреть подходы обнаружения и исправления ошибок, имеющих следующую по величине оценку.

В основе разрабатываемого программного средства, реализующего выбранные подходы, лежит логика кода Хемминга.

Целью экспериментального исследования является реализация подхода по обнаружению и исправлению ошибок передаваемых данных. Для достижения поставленной цели была проведена серия из трех групп экспериментов по передаче данных. В первом случае зашифрованное для передачи сообщения соответствовало передаваемому. Во второй контрольной группе зашифрованное сообщение не соответствовало передаваемому, при передаче была допущена одна ошибка. В третьей группе экспериментов осуществлялась передача сообщения, не соответствующего зашифрованному на более чем одну ошибку. Результаты эксперимента представлены в таблице 1.

Таблица 1

Результаты экспериментального исследования

№	Название эксперимента	Входные данные	Полученный результат
1	Передача данных без ошибок	Зашифрованное сообщение: 00010111 Передаваемое сообщение: 00010111	Передаваемые данные соответствуют полученным. Ошибок не обнаружено
2	Передача данных с одной ошибкой	Зашифрованное сообщение: 00010111 Передаваемое сообщение: 00000111	Передаваемые данные соответствуют полученным. Обнаружена и исправлена одна ошибка.

Окончание таблицы 1

№	Название эксперимента	Входные данные	Полученный результат
3	Передача данных более чем с одной ошибкой	Зашифрованное сообщение: 00010111 Передаваемое сообщение: 00001111	Передаваемые данные не соответствуют полученным. Обнаружено более одной ошибки, исправление ошибок не является возможным.

При реализации первой группы экспериментов ошибок в передаваемых данных не было обнаружено так как зашифрованное для передачи сообщение полностью соответствовало передаваемому, и передача осуществлялась без потерь данных. При передаче данных с одной ошибкой (вторая группа экспериментов) разработанное программное средство обнаруживало и исправляло ее. В результате передаваемые данные соответствовали полученным. Третья группа экспериментов показала, что при наличии в передаваемом сообщении более чем одной ошибок их исправление не является возможным.

Список литературы

1. ГОСТ Р 58412-2019 Защита информации. РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. Угрозы безопасности информации при разработке программного обеспечения: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 19 августа 2015 г. № 1181-ст. (дата обращения 15.10.2021).

2. ФСТЭК. БАЗОВАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ. УТВЕРЖДЕНА Заместителем директора ФСТЭК России 21 мая 2019 г. (дата обращения: 15.10.2021).

3. Желобанов Д. Б. НАДЕЖНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. URL: https://elar.urfu.ru/bitstream/10995/45540/1/nt-10-1-2006-071.pdf (дата обращения: 15.10.2021).

4. Шубинский, И.Б. МЕТОДЫ ОБЕСПЕЧЕНИЯ ФУНКЦИОНАЛЬНОЙ НАДЕЖНОСТИ ПРОГРАММ. URL: http://www.ibtrans.ru/upload/iblock/c44/c44620b0cb7906c2abb378a9ae9e7d6c.pdf (дата обращения: 15.10.2021).

СРАВНЕНИЕ МЕТОДОВ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Бережная Дарья Андреевна

Студент кафедры информационной безопасности,

Волгоградский государственный университет

просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Пономарев Михаил Витальевич

Студент кафедры информационной безопасности,

Волгоградский государственный университет

просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Рассматриваются и анализируются методы биометрической аутентификации. Приводится характеристика методов биометрической аутентификации.

Ключевые слова: биометрия, аутентификация, биометрическая аутентификация, анализ, метод, отпечаток пальца, зрачок, отпечаток ладони.

COMPARISON OF BIOMETRIC AUTHENTICATION METHODS

Berezhnaya Daria Andreevna

Student of Department of Information Security,

Volgograd State University

Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation

Ponomarev Mikhail Vitalievich

Student of Department of Information Security,

Volgograd State University

Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation

Abstract. Biometric authentication methods are considered and analyzed. The characteristics of biometric authentication methods are given.

Key words: biometrics, authentication, biometric authentication, analysis, method, fingerprint, pupil, palm print.

Защита конфиденциальной информации имеет первостепенное значение в современном цифровом мире из-за доступа злоумышленников к уязвимостям. В настоящее время в цифровом обществе растет кража цифровой информации. Кроме того, выявление и смягчение последствий такого рода операций является проблемой. Для этого регистрация пользователей должна проходить таким образом, чтобы снизить возможность несанкционированного доступа к личным данным до минимума.

Регистрация пользователя в любой системе выполняется через три этапа, следующих друг за другом: идентификацию, аутентификацию и авторизацию соответственно. В статье рассматривается второй этап, то есть процедура аутентификации. Удостоверение личности человека часто проводится, используя характерные только этому человеку признаки. Такая технология основана на использовании знаний биометрии (биометрики). Под биометрией понимается набор уникальный характеристик отдельного субъекта, таких как физиологические или поведенческие, которые не изменяются со временем. В физиологические характеристики включаются отпечатки пальцев, изображение зрачка, рук, лица и других, а в поведенческие – рукописная подпись, голос, походка, стиль печати на клавиатуре и другое. Биометрия играет огромную роль в идентификации и удостоверении личности индивидуума. На рисунке 1 показаны существующие биометрические характеристики, используемые в системах аутентификации.

Для сравнения различных биометрических технологий определим критерии сравнения: Сложность подделки признака (К1), Статичность признака (К2), Простота анализа (К3), Простота сбора (К4), Стойкость по отношению к ложному срабатыванию (К5), Стоимость (К6).

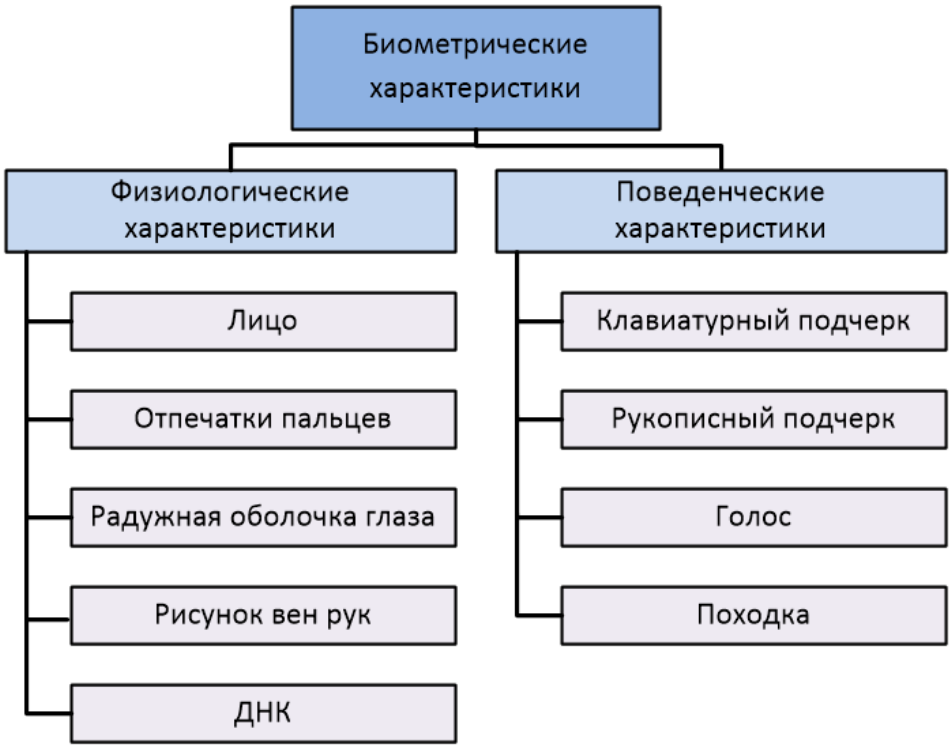

Рис. 1. Биометрические характеристики и их классификация

Также введем численные показатели критериев, где 0 – соответствует низким показателям признака, 0.5 – средним показателям и 1 – высоким показателям.

В таблице 1 приведены сравнения биометрических характеристик на основе выбранных критериев.

В ходе анализа выяснилось, что данные ДНК, радужной оболочки глаза и отпечатка пальца являются самыми безопасными, а биометрические данные по голосу и лицу пользовались самым высоким уровнем принятия пользователями, что повлияло на показатель простоты сбора. Несмотря на все это, именно биометрические данные по отпечатку пальца являются лучшим решением в целом.

Биометрическая технология широко применяется и принята во всем мире для аутентификации личности индивидуума. Также применяемая технология преодолевает ограничения, с которыми сталкивается традиционный процесс аутентификации, такие как проблемы, основанные на знаниях, включая пароль и токен для аутентификации человека.

Таблица 1

Сравнение биометрических характеристик
на основе выбранных критериев

Биометрическая характеристика	**K1**	**K2**	**K3**	**K4**	**K5**	**K6**	**Результирующий столбец**
Лицо	1	0,5	0,5	1	0,5	0,5	**4**
Отпечаток пальца	1	1	0,5	0,5	1	0,5	**4,5**
Радужная оболочка глаза	1	1	0	0,5	1	0,5	**4**
Рисунок вен рук	0,5	1	0,5	0,5	0,5	0,5	**3,5**
ДНК	1	1	0	0	1	0	**3**
Клавиатурный подчерк	0	0	0,5	1	0,5	1	**3**
Рукописный подчерк	0	0,5	0,5	0,5	0	1	**2,5**
Голос	0,5	0,5	0,5	1	0,5	0,5	**3,5**
Походка	1	0,5	0	0,5	0,5	0,5	**5**

Изучение и развитие биометрических систем является очень важным шагом для развития безопасности данных и личности пользователей. В данный момент наиболее безопасным методом идентификации и аутентификации человека является совместное использование нескольких методов, например, пароля вместе с отпечатком пальца, но в дальнейшей перспективе возможно будет создать такую биометрическую систему, которая быстро и без ошибок сканирует сразу несколько биометрических характеристик, не требуя от пользователя знания пароля, который легко взломать, забыть, или потерять.

Список литературы

1. Аутентификация. Теория и практика. Под ред. проф., д.т.н. Шелупанова. М.: Горячаялиния-Телеком, 2009,- 552 с.

2. Choudhury B, Then P, Issac B, Raman V and Haldar M K, “A Survey on Biometrics and Cancelable Biometrics Systems”, International Journal of Image and Graphics, pp. 1-28, 201

3. Gursimarpreet Kaur and Chander Kant Varma, “Comparative Analysis of Biometric Modalities”, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 4, pp. 603-613, 2014.

БЕЗОПАСНАЯ КОМПИЛЯЦИЯ И АРХИТЕКТУРЫ ЗАЩИЩЕННЫХ МОДУЛЕЙ

Дегтярев Даниил Игоревич

Студент кафедры информационной безопасности,

Волгоградский государственный университет

просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Какорина Олеся Александровна

Кандидат физико-математических наук,

заведующий кафедрой информационной безопасности

Волгоградского государственного университета

просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Поднимается вопрос представления системы в виде иерархии уровней абстракции. Рассматриваются возможные решения построения архитектуры защищенных модулей программного обеспечения.

Ключевые слова: абстракция, безопасная компиляция, информационная безопасность, защита данных.

SECURE COMPILATION AND SECURE MODULES ARCHITECTURE

Degtyarev Daniil Igorevich
Student of Department of Information Security,
Volgograd State University
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation
Kakorina Olesya Alexandrovna
Candidate of Physico-mathematical Sciences,
Head of the Department of Information Security,
Volgograd state University
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation

Abstract. The question of representing the system as a hierarchy of abstraction levels is raised. Possible solutions for constructing the architecture of protected software modules are considered.

Key words: abstraction, safe compilation, information security, data protection.

Абстракция является важным методом управления сложностью компьютерных систем. Декларативные операторы в программе используются для сокрытия деталей, которые не имеют значения на определенном уровне абстракции. Однако, когда предположения и интуитивные свойства абстракции не соответствуют конкретной реализации, это может привести к уязвимостям безопасности, которые могут быть использованы злоумышленниками, взаимодействующими с приложением на уровне реализации.

Разработчики программного обеспечения обычно рассуждают о свойствах приложения на высокий уровень абстракции. Основную причину большого числа уязвимостей программного обеспечения часто можно объяснить, как высокоуровневую абстракцию в программном приложении, которая может быть нарушена в представлении этого приложения более низкого уровня. Знакомые абстракции программирования, такие как процесс,

модуль, функция, стек, тип и лексическая область видимости, часто существуют только в исходном коде или реализованы таким образом, чтобы не применять абстракцию, о которой идет речь. Однако недавние исследования показали, что свойства безопасности, выраженные в исходном коде приложения могут быть сохранены даже после того, как это высокоуровневое представление было преобразовано в машинный код низкого уровня. Область безопасной компиляции изучает схемы компиляции, которые выполняют преобразования в объекты программного обеспечения, в результате которых представления являются такими же безопасными, как и их исходный код. Компилятор с этим свойством позволяет рассуждать о безопасности приложения на уровне абстракции исходного кода.

Защита памяти – это хорошо зарекомендовавший себя метод защиты, при котором память компьютерной системы разделяется на несколько сегментов. Доступ к отдельным сегментам затем управляется в соответствии с политикой безопасности, обычно выражаемой в терминах некоторых абстракций более высокого уровня, таких как изоляция, процесс и модуль. Например, изоляция компьютерных процессов предотвращает доступ одного компьютерного процесса к сегментам памяти, выделенным другим процессам. В обычных компьютерных системах изоляция процессов обычно реализуется с помощью отдельных адресных пространств посредством тесное сотрудничество между всемогущим монолитным ядром и компьютерным оборудованием.

Архитектура защищенных модулей (PMA) – это новый класс архитектур безопасности с более тонкой схемой защиты памяти для защиты небольших изолированных отсеков, которые совместно используют адресное пространство. Эти архитектуры позволяют разработчикам программного обеспечения создавать "анклав" в общем адресном пространстве для защиты от потенциально вредоносной окружающей среды. Такой анклав характеризуется защищенным разделом кода, защищенным разделом данных и ограниченным числом взаимодействий между изолированным модулем и

заключающим приложением. PMA предотвращает несанкционированный доступ к разделам памяти анклава и гарантирует, что изолированный модуль может быть вызван исключительно через одну из его точек взаимодействия, что напоминает концепции разработки программного обеспечения, такие как сокрытие информации и интерфейсы.

PMAS может гарантировать свойства изоляции защищенного модуля (PM), даже если заключающее приложение было скомпрометировано злоумышленником.

PMA на основе аппаратного обеспечения продвигают эту идею на шаг дальше и также могут исключить операционную систему (ОС) из доверенной вычислительной базы приложения (TCB), набор аппаратных и программных компонентов, которым необходимо доверять, не содержат никаких уязвимостей в системе безопасности. Чем больше УТС, тем больше вероятность того, что он содержит дыры в безопасности, которые могут быть использованы и тем сложнее доказать, что приложение является правильным и безопасным.

Список литературы

1. Джеймс Фостер, Майк Прайс. Защита от взлома: сокеты, эксплойты, shell-код = Sockets, Shellcode, Porting, &Coding. – М.: Издательский Дом ДМК-пресс, 2006. – С. 35, 532. – 784 с. – ISBN 5-9706-0019-9.

2. Clang: A C language family frontend for LLVM. https://clang.llvm.org. Accessed: 2018-06-03.

3. Extending LLVM: Adding instructions, intrinsics, types, etc. https://llvm. org/docs/ExtendingLLVM.html. Accessed: 2018-06-03.

4. Intel Software Guard Extensions (Intel SGX) SDK. https://software.intel. com/en-us/sgx-sdk. Accessed: 2018-06-03.

ОЦЕНКА ЗАЩИЩЕННОСТИ РЕЧЕВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ

Дудакова Елизавета Сергеевна
магистрант кафедры информационной безопасности
Волгоградского государственного университета
infsec@volsu.ru
Проспект Университетский, 100, 400062 г. Волгоград, Российская Федерация
Никишова Арина Валерьевна
кандидат технических наук
доцент кафедры информационной безопасности
Волгоградского государственного университета
nikishova.arina@volsu.ru
Проспект Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Значимость речевой информации для организации никак не меньше информации на других носителях. И для этого вида информации также встает вопрос комплексной оценки ее защищенности, учитывающей различные факторы, влияющие на нее. Предлагается подход к оценке защищенности речевой информации от утечки с учетом показателей разборчивости речи и характеристик потенциального злоумышленника.

Ключевые слова: речевая информация, злоумышленник, разборчивость речи, защищенность, угроза безопасности.

ASSESSMENT OF SPEECH INFORMATION SECURITY FROM LEAKAGE

Dudakova Elizaveta Sergeevna
master's student of Department of information security,
Volgograd State University
infsec@volsu.ru
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation

Nikishova Arina Valerevna
Candidate of technical sciences
Associate professor of Department of information security,
Volgograd State University
nikishova.arina@volsu.ru
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation

Abstract. The importance of speech information for the organization is no less than of information on other media. And for this type of information, there is also a question of a comprehensive assessment of its security, taking into account various factors affecting it. The approach is proposed to assess the security of speech information from leakage, taking into account the indicators of speech intelligibility and characteristics of a potential intruder.

Key words: speech information, intruder, speech intelligibility, security, security threat.

Речевая информация имеет большое значение для организации. Обеспечение безопасности переговоров и совещаний – одно из важных направлений защиты информации. При этом, как и для остальных направлений обеспечения информационной безопасности, ключевым моментом является оценка качества примененных мер и средств защиты через итоговую оценку защищенности речевой информации от утечки.

При проведении в организации переговоров или совещаний, на которых обсуждается информация ограниченного доступа, возникают угрозы безопасности речевой информации:

— подслушивание с использованием специального, в том числе и скрытого, оборудования;

— несанкционированная запись с использованием специального, в том числе и скрытого, оборудования;

— перехват информации на неконтролируемой территории с помощью специального оборудования;

— перехват побочных электромагнитных излучений, возникающих при работе звуковых устройств и другого оборудования.

Тогда необходимо обеспечить защиту речевой информации:

— в защищаемом помещении;

— в системах звукового сопровождения и звукоусиления;

— при проведении звукозаписи;

— при передаче по незащищенным каналам связи.

При этом необходимо учесть такие характеристики как:

— категория лиц, к которой можно отнести злоумышленника;

— мотивы и цели нарушителя;

— уровень квалификации злоумышленника;

— уровень оснащенности злоумышленника.

Основным показателем защищенности речевой информации является ее разборчивость при перехвате злоумышленником. При этом разделяют слоговую и словесную разборчивость.

Предлагается оценивать защищенность речевой информации от утечки с учетом показателей разборчивости речи и характеристик потенциального злоумышленника. Тогда оценка защищенности речевой информации имеет вид (рисунок 1).

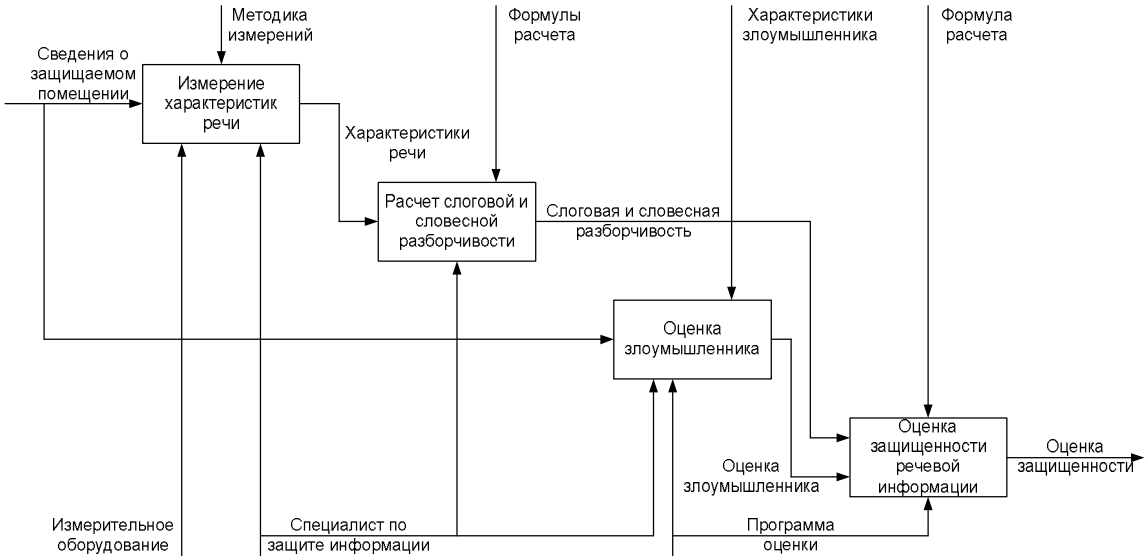

Рис. 1. IDEF0-диаграмма оценки защищенности речевой информации от утечки

Следуя предложенной функциональной модели, можно оценить не просто разборчивость речи, но и учесть при этом характеристики потенциальных злоумышленников.

Список литературы

1. Титов М.Ю., Журавлев С.И., Ершов Н.С., Костина Н.М. Проблемы и перспективы защиты акустической речевой информации // Промышленные АСУ и контроллеры. 2021. № 2. С. 55–58.

2. Моисеева М.В., Фурсова А.В. Система защиты информации от утечки по акустическим каналам на основе речеподобной помехи // Материалы Международной (заочной) научно-практической конференции «Инновационные процессы в научной среде». 2021. С. 78–84.

3. Рыбалкин О.Д., Ромашко Б.В. К методике оценки защиты информации // Наука и образование сегодня. 2020. № 4 (51). С. 9–11.

ОБЗОР МЕТОДОВ АНАЛИЗА ВРЕДОНОСНЫХ ПРОГРАММ

Ермашкевич Екатерина Александровна

Студент кафедры информационной безопасности,

Волгоградский государственный университет

просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Головачева Наталья Алексеевна

старший преподаватель кафедры информационной безопасности,

Волгоградский государственный университет

golovacheva.natalya@volsu.ru

просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Проводится анализ методов вредоносных программ. Выделяются ключевые особенности статического, динамического, гибридного и анализа памяти.

Ключевые слова: анализ вредоносных программ, память данных, информационная безопасность, защита данных.

OVERVIEW OF MALWARE ANALYSIS METHODS

Ermashkevich Ekaterina Alexandrovna
Student of Department of Information Security,
Volgograd State University
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation
Golovacheva Natalia Alekseevna
Senior lecturer of Department of information security,
Volgograd state University
golovacheva.natalya@volsu.ru
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation

Abstract. Malware methods are being analyzed. The key features of static, dynamic, hybrid and memory analysis are highlighted.

Key words: malware analysis, data memory, information security, data protection.

Анализ вредоносных программ – это процесс понимания поведения и назначения определенного образца вредоносных программ для выявления и оценки угроз.

Существует 4 вида методов, используемых для анализа вредоносных программ:

1. Статический анализ – это процесс анализа скомпилированного файла вредоносной программы без запуска кода.

Выполняется путем определения сигнатуры двоичного файла вредоносной программы. Расчет криптографического хэша двоичного файла и понимание каждого из его компонентов помогает определить его подпись. Исполняемый файл двоичного файла вредоносной программы загружается в дизассемблер и, таким образом, исполняемый машиной код преобразуется в код языка ассемблера. Таким образом, выполняя обратное проектирование двоичного файла вредоносного ПО, аналитику становится легко его читать и понимать.

Также данный метод условно можно разделить на базовый и продвинутый анализ:

– Базовый статический анализ – это процесс анализа скомпилированного файла вредоносного ПО исключая просмотр самого кода.

– Продвинутый статический анализ – это процесс изучения кода вредоносной программы полученного методом обратной разработки.

2. Динамический анализ заключается в запуске образца вредоносного программного обеспечения и наблюдении за его поведением в системе, чтобы удалить последствия его работы или остановить распространение вредоносного программного обеспечения на другие системы. Система настроена в изолированной виртуальной среде, поэтому образец можно изучать без риска повреждения основной операционной системы.

Во время динамического анализа вредоносных программ при запуске кода индикаторы предоставляют сигнатуру обнаружения, которую можно идентифицировать только с помощью динамического анализа. Техника определения поведения ищет следующее:

– Анализ сетевого трафика.

– Поведение файловой системы.

– Изменения в реестре.

Метод динамического анализа, также, как и метод статического анализа можно разделить на базовый и продвинутый анализ:

– Базовый динамический анализ – это процесс, при котором происходит запуск вредоносной программы в изолированной виртуальной среде и наблюдение за ее поведением в системе.

– Продвинутый динамический анализ происходит с использованием специализированного отладчика, который позволяет исследовать внутреннее состояние запущенной вредоносной программы.

3. Гибридный анализ собирает информацию о вредоносных программах с помощью статического и динамического анализа. Используя

гибридный анализ, исследователи безопасности получают преимущества как статического, так и динамического анализа. Таким образом, повышается способность правильно обнаруживать вредоносные программы, и преодолевает ограничения методологии статического или динамического анализа вредоносных программ.

Гибридный анализ анализирует спецификацию сигнатур любого вредоносного кода. Затем он объединяет его с другими поведенческими параметрами. Это для улучшения методологии анализа вредоносных программ.

4. Анализ памяти дает всесторонний анализ вредоносных программ, поскольку исследует вредоносные крючки и код за пределами нормальной области действия функции. Он использует образ памяти для анализа информации о запущенных программах, операционной системе и общем состоянии компьютера.

В памяти можно найти значительный объем информации, такой как активные и завершенные процессы, библиотеки динамических ссылок (DLL), запущенные службы, реестр и активные сетевые подключения. Кроме того, изучение памяти может обнаружить методы подключения процессов/ DLL, используемые вредоносными программами, чтобы выглядеть как законный процесс.

Анализ предоставляет точную информацию о поведении вредоносных программ путем извлечения функций на основе памяти, которые могут выражать действия и характеристики вредоносных программ.

Список литературы

1. Гордон Я., Компьютерные вирусы без секретов. – М.: Новый издательский дом, 2004. – с. 320.

2. J. Okolica and G. Peterson, “A compiled memory analysis tool,” in IFIP Advances in Information and Communication Technology, 2010, vol. 337 AICT, pp. 195–204.

3. MeringM., Childers S., Fleming A. Report of Task Force on Metadata Analysis // American Library Association. – Lincoln, 2006. – C. 17.

ИССЛЕДОВАНИЕ СПОСОБОВ ОБНАРУЖЕНИЯ ПРОГРАММНЫХ ЗАКЛАДОК

Жуйков Егор Андреевич
Студент кафедры информационной безопасности,
Волгоградский государственный университет
27egor@gmail.com
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация
Никишова Арина Валерьевна
К.т.н., доцент кафедры информационной безопасности,
Волгоградский государственный университет
nikishova.arina@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В данной статье рассматриваются основные способы обнаружения программных закладок, выделяются критерии выбора наиболее лучшего способа обнаружения программных закладок, проводится анализ способов обнаружения программных закладок по выделенным критериям.

Ключевые слова: конфиденциальная информация, злоумышленник, программные закладки, безопасность, вредоносное ПО.

STUDY OF METHODS FOR DETECTING SPYWARE

Zhuikov Egor Andreevich
Student of Department of Information Security,
Volgograd State University
27egor@gmail.com
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation

Nikishova Arina Valerievna
Candidate of Technical Sciences,
Associate Professor of Department of Information Security
Volgograd Staty University
nikishova.arina@volsu.ru
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation

Abstract. This article discusses the main methods for detecting software bugs, highlights the criteria for choosing the best way to detect software bugs, analyzes the methods for detecting software bugs according to the selected criteria.

Key words: confidential information, penetration, spyware, security, malware.

В современном обществе одним из распространенных источников получения конфиденциальной информации является компьютерные сети. Большое количество компаний имеют свои собственные страницы в сети, так же их подразделения используют компьютерную сеть для обмена конфиденциальной информации. Главной задачей компаний является защита конфиденциальной информации от несанкционированного доступа, для этого они используют целый комплекс технических, программно-аппаратных средств и административных мер защиты информации.

Утечка конфиденциальной информации организации наносит непоправимый ущерб репутации организации, который приводит за собой финансовые убытки. Одним из методов получения конфиденциальной информации являются программные закладки. Для того чтобы обнаружить программные закладки на рабочем месте существуют различные способы. Целью данной статьи является выбор наиболее подходящего способа обнаружения программах закладок.

По данным статистического исследования компании Positive Technologies за 2020 года количество инцидентов с использованием стороннего ПО, по сравнению с 2019 годом, выросло на 54%, из них:

шпионское ПО (24% у организаций, 50% у частных лиц), ВПО для удаленного управления (18% у организаций, 16% у частных лиц), загрузки (12% у организаций, 14% у частных лиц), троян (11% у организаций, 22% у частных лиц), рекламное ПО (1% у организаций, 13% у частных лиц). Большинство инцидентов утечек информации происходит с помощью программных закладок, в связи с этим необходимо выполнять регулярную проверку системы на наличие программных закладок.

Для определения наиболее подходящего способа обнаружения программных закладок рассмотрим все существующие способы обнаружения программных закладок, определим критерии и проведем сравнительный анализ по выделенным критериям.

Для выявления в системе программах закладок могут применятся следующие способы:

1. Качественный и визуальный [2, 3].

Данный способ основывается на ощущениях и наблюдениях пользователя КС, таких как высокая нагрузка на центральном процессоре и оперативной памяти, высокая нагрузка на сеть, изменения состава файлов и длинны файлов. Несмотря на то что мнение об признаках этого способа субъективны, тем не менее, они часто свидетельствуют о наличии в системе неполадок или ошибок, что требует проведения проверок на наличие программных закладок.

2. Обнаружение средствами тестирования и диагностики [2, 3].

Данный способ характерен как для программных закладок, так и для выявления программных вирусов, его суть заключается в автоматическом нахождении вредоносного кода, просмотра активных процессов, просмотра состояния IP-портов, просмотра разделов реестра на наличие установленных дополнительных программ, просмотр файлов аудита. Например, антивирусные программы успешно справляются с обнаружением загрузочных закладок, определять статические ошибки на диске хорошо помогает средство Disk Doctor, а для проверки целостности данных на диске средство Adinf.

Определим критерии для оценки способов обнаружения программных закладок:

Критерий 1. Объем. Данный критерий определяет объем обрабатываем информации.

Критерий 2. Автоматическое нахождение. Данный критерий определяет уровень способ нахождения программной закладки.

Критерий 3. Использование стороннего ПО. Данный критерий определяет возможность использовать стороннее ПО, для нахождения программной закладки.

Критерий 4. Время. Данный критерий определяет время нахождения программной закладки.

Критерий 5. Надежность. Данный критерий определяет уровень надежности способа обнаружения программной закладки.

Проведем сравнительный анализ способов обнаружения программных закладок по выделенным критериям. В таблице представлены обозначения «1» – критерий выполняется, «0» – критерий не выполняется.

Таблица 1

Сравнительный анализ способов обнаружения программных закладок

Способ / Критерий	Качественный и визуальный	Обнаружение средствами тестирования и диагностики
Объем	0	1
Автоматическое нахождение	0	1
Использование стороннего ПО	1	1
Время	1	0
Надежность	0	1
Итог	0,4	0,8

По результатам сравнительного анализа способов обнаружения программных закладок по выделенным критериям, выявлено, что наиболее подходящим способом является «Обнаружение средствами тестирования и диагностики.

Список литературы

1. Актуальные киберугрозы: итоги 2020 года. // Positive Technologies [Сайт]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/

2. Способы обнаружения присутствия программных закладок // Taketop [Сайт]. – URL: http://taketop.ru/articles/infor-bezop/zashitakompin/sposobu-obnar

3. Методы защиты от программных закладок // Helpiks.org [Сайт]. – URL: https://helpiks.org/9-27388.html

ОБЗОР МЕТОДОВ РАСПОЗНАВАНИЯ ЛИЦ

Ковтунова Анна Александровна

Студент кафедры информационной безопасности,

Волгоградский государственный университет

просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Попов Глеб Александрович

Старший преподаватель кафедры информационной безопасности,

Волгоградский государственный университет

gpopov@volsu.ru

просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. За последние два десятилетия проводится множество исследований в области распознавания объектов, сопоставления форм и распознавания образов в области компьютерного зрения. Распознавание лиц – одна из важных задач в распознавании объектов и компьютерном зрении. В нашей повседневной деятельности доступен ряд биометрических приложений для распознавания людей, таких как распознавание глаз или

радужной оболочки глаза, распознавание отпечатков пальцев, распознавание лиц. Лицо является важной частью человеческого существа и требует обнаружения для различных приложений, таких как безопасность, судебная экспертиза. Для этого требуются надлежащие методы обнаружения и распознавания лиц с различными выражениями лица, вариацией позы, окклюзии, старения и разрешения либо в кадре неподвижного объекта, либо в видеопоследовательности изображений. В данной статье автор постарался предоставить анализ всех методов распознавания лиц, что должно значительно облегчить выбор наиболее подходящего для определенного случая.

Ключевые слова: распознавание лиц, анализ, методы, идентификация.

OVERVIEW OF FACE RECOGNITION METHODS

Kovtunova Anna Alexandrovna
Student of Department of Information Security,
Volgograd State University
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation
Popov Gleb Alexandrovich
Senior Lecturer of the Department of Information Security of
Volgograd state University
gpopov@volsu.ru
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation

Abstract. Over the past two decades, a lot of research has been carried out in the field of object recognition, shape matching and pattern recognition in the field of computer vision. Face recognition is one of the important tasks in object recognition and computer vision. A number of biometric applications for human recognition are available in our daily activities, such as eye or iris recognition, fingerprint recognition, face recognition. The face is an important part of the human being and requires detection for various applications such as security, forensics. This requires proper methods for detecting and recognizing faces with

different facial expressions, pose variation, occlusion, aging, and resolution, either in a still object frame or in a video image sequence. In this article, the author has tried to provide an analysis of all face recognition methods, which should greatly facilitate the choice of the most appropriate for a particular case.

Key words: Face recognition, analysis, methods, identification.

Распознавание лиц – всегда интересная область и одна из сложных задач компьютерного зрения и поиска изображений. В настоящее время оно применяется в различных областях, таких как банкоматы, система здравоохранения, система водительских прав, наблюдение и аутентификация паспорта. В большой базе данных распознавание изображений лиц всегда является сложной задачей. Существуют различные биометрические функции, которые могут использоваться для идентификации человека, такие как активное сотрудничество человека для аутентификации, тогда как распознавание лиц не требует активного сотрудничества человека. Таким образом, распознавание лиц намного удобнее по сравнению с другими биометрическими данными. Очень важно определить значение данного термина. Распознавание лица – это технология, которая позволяет идентифицировать или верифицировать определенного человека. Для этого используют нейросети, которые умеют считывать и анализировать уникальные черты лица и сверять их с базой. Данные важные задачи так же называют проверкой и идентификацией. Подтверждение лица может быть определено как однозначное совпадение, при котором изображение лица сопоставляется с доступным банком данных изображений лиц, личность которого сопоставляется. Идентификация лица – это проблема один к N, которая сопоставляет изображение лица в запросе с доступным изображением в базе данных лиц. Также рассматривается третий случай, когда лицо запроса может быть или не быть в доступной базе данных. В таком случае можно вычислить оценку сходства и на основе наивысшей оценки сходства можно найти совпадение. Для решения данной задачи был

изучен ряд методов распознавания лиц в 2D и 3D и предложен инфракрасный спектр (IRS) для решения проблем распознавания лиц. Обнаружение и сопоставление лиц важны для выделения черт лица и расчета точности. Распознавание лиц по-прежнему является проблемой для распознавания лиц в движущихся изображениях, близнецов, вариаций позы, наличия различных аксессуаров, таких как борода, очки, цвет волос, перегородка для волос, макияж, различные выражения лица при разных условиях освещения, интенсивности света, шума, окклюзии для сопоставления лиц и генерации ошибок. Для этого обратили внимание на различные методы распознавания лиц (FER) на основе геометрии и внешнего вида, был проведен сравнительный анализ различных методов извлечения признаков на основе набора данных JAFFE.

Человека можно идентифицировать с помощью различных черт лица, отпечатка пальца, глаза или радужной оболочки, строения тела, родимого пятна и так далее. Лицо – одна из важных частей тела, которая играет важную роль в распознавании людей. Разрешение играет жизненно важную роль в распознавании лиц при распознавании лиц при наблюдении. В системе распознавания лиц первым шагом является обнаружение лица на изображении. Для распознавания лица разбиваются на четыре основные части, такие как глаза, губы, рот и нос. Основная задача обнаружения лиц – определить количество лиц на изображении, учитывая неподвижное изображение. Лица в основном размещаются в 2D или 3D с разными текстурами и мимикой.

1. 2D распознавание лиц

Ранее для двухмерного распознавания лиц использовались следующие четыре шага: обнаружение лица, выравнивание лица, извлечение признаков и сопоставление признаков из базы данных зарегистрированных пользователей для распознавания лица. Матрица была рассчитана на основе значений пикселей в углу лица при различных условиях освещения для 2D-распознавания. Обычно изображения лиц представлены многомерным

вектором, содержащим значения пикселей. Сопоставление функций выполняется для сопоставления лица в виде изображения или видео из доступной базы данных зарегистрированных изображений с уникальной идентификацией лица. Различные методы, принятые для распознавания лиц, основывались на цвете, интенсивности и освещении. Исследователь сталкивается со многими проблемами, такими как выражение лица, освещение, вариации ориентации изображения и окклюзия при распознавании лиц. В данном методе существуют некоторые ограничения. В системе распознавания лиц 2D скорость и производительность зависят от захвата изображения при таких условиях как: ориентация головы, качество изображения, условия освещения, частичная окклюзия, мимика.

2. 2D-3D распознавание лиц:

Андреа Ф. Абате и др. предложили надежный метод коллективного распознавания лиц в 2D визуальных изображениях и 3D-моделях на основе различных параметров, в которые входят: размер исходных данных, количество решаемых задач и скорость распознавания. Сравнение различных методов открывает перед исследователями перспективу использования новых методов в области распознавания лиц. Методы стереозрения, используемые для повышения производительности системы распознавания двухмерных лиц с трехмерной информацией известно, как несоответствие лиц. Лицо человека в другом положении было сопоставлено с помощью нейронной сети на основе сканируемых линий. Анализ главных компонентов (PCA) для извлечения признаков и идентификации эффективно использовался для распознавания лиц. Скорость распознавания лиц 2D- 3D была улучшена за счет добавления информации глубины.

3. 3D распознавание лиц

Лица представлены в виде реального изображения, различной текстуры, разного каркаса, свернутого в трех измерениях. Это кажется более точным распознаванием изображения лица и минимизацией проблемы вариаций позы, окклюзии и различного состояния освещения.

С. Солтанпура и другие предложили исследование для трехмерного распознавания лиц на основе местных особенностей. Они разделили локальный дескриптор на кривые, ключевые точки и поверхность. Они применили технологию получения изображений в базе данных трехмерных лиц для сравнения в различных условиях. Извлечение признаков – один из важных модулей в распознавании лиц, который рассматривался авторами. Они изучали различные типы дескрипторов лица и функции для 3D-распознавания лиц. Они также рассмотрели проблемы распознавания лиц с различным выражением лица и окклюзиями. При извлечении 3D-изображения и черт лица используются различные техники и методы для эффективного распознавания. Нормализация между зондом и текстурой галереи выполняется с помощью двунаправленного повторного освещения. Внедрение показателей корреляции для определения оценок сходства и концепции позы и нормализованных сигнатур света для проверки лиц часто довольно популярно. Мотивация к использованию технологии распознавания лиц 3D заключается в преодолении недостатков систем распознавания лиц в 2D. Трехмерные изображения лиц распознавались с помощью различных техник аугментации и тестировались на различных базах данных. Он был усовершенствован с помощью опытной сенсорной камеры, обеспечивающей лучшее трехмерное изображение лица, которое может создавать трехмерные модели лица. Доступны различные методы распознавания 3D-лица с разных углов обзора. Одним из преимуществ системы распознавания лиц 3D является то, что на нее не влияет сила света. Было введено несколько методов для извлечения признаков, чтобы повысить точность и скорость распознавания. Джи Вен и другие предложили улучшенное распознавание лиц с адаптацией домена. В этой статье авторы попытались оценить распознавание лиц, взяв набор данных «Помеченные лица в дикой природе» (LFW) в качестве ориентира.

В конце нашего анализа мы можем сделать вывод, что лицо – важнейшая характеристика живого тела, играющая важную роль в узнавании

человека. В приложениях и исследованиях распознавания лиц по всему миру используются различные методы. В этой статье автор попытался расширить обзор методов распознавания лиц. Распознавание лиц имеет все более широкую область применения, например, в области безопасности и криминалистики, и требует большей точности и надежности. Именно поэтому очень важно иметь представление о всех методах для выбора, наиболее подходящего для распознавания лиц.

Список литературы

1. Andrea F. Abate, Michele Nappi, Daniel Riccio, Gabriele Sabatino. (2007) “2D and 3D face recognition: A survey” Pattern Recognition Letter s 28(14): 1885-1906.

2. Ge Wen, Huaguan Chen, Deng Cai, Xiaofei He. (2018),” Improving face recognition with domain adaptation”, Neurocomputing 287: 45-51.

3. Ioannis A. Kakadiaris, George Toderici, Georgios Evangelopoulos, Georgios Passalis, Theoharis. (2017) “3D-2D face recognition with pose and illumination normalization” Computer Vision and Image Understanding 154:137-151.

4. Jyoti Kumar, R.Rajesh, KM.Pooja. (2015) “Facial expression recognition: A survey” Procedia Computer Science 58: 486 – 491.

5. Shwetank Arya, NeerajPratap, Karamjit Bhatia. (2015) “Future of Face Recognition: A Review” Procedia Computer Science 58:578 – 585.

К ВОПРОСУ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ХРАНИЛИЩ [1]

Корх Ирина Анатольевна

Старший преподаватель кафедры КТиИБ,

Кубанский государственный технологический университет,

Московская ул., 2, 350072 г. Краснодар, Краснодарский край,

Российская Федерация

aia2004@inbox.ru

Маврешко Вячеслав Михайлович
Студент,
Кубанский государственный технологический университет,
Московская ул., 2, 350072 г. Краснодар, Краснодарский край,
Российская Федерация
slavamavreshko@yandex.ru

Аннотация. В статье рассмотрены последовательность действий при отправке данных в «облако» и возможные варианты обеспечения безопасности информации на каждом из этапов. Также были предложены способы, методы и средства по защите информации при входе в облачное хранилище и на протяжении хранения в нем информации.

Ключевые слова: облачное хранилище, средство защиты информации, криптография, биометрическая аутентификация.

ON THE ISSUE OF CLOUD STORAGE SECURITY [1]

Korkh Irina Anatolievna
Senior Lecturer
Kuban State Technological University,
Moskovskaja ul., 2, 350072 g. Krasnodar, Krasnodarskij kraj,
Russian Federation
aia2004@inbox.ru
Mavreshko Viacheslav Mikhailovich
Student
Kuban State Technological University,
Moskovskaja ul., 2, 350072 g. Krasnodar, Krasnodarskij kraj,
Russian Federation
slavamavreshko@yandex.ru

Abstract. The article discusses the sequence of actions when sending data to the cloud and possible options for ensuring the security of information at each stage. Methods, methods and tools for protecting information when

logging into the cloud storage and during the storage of information in it were also proposed.

Key words: cloud storage, information security tool, cryptography, biometric authentication.

В последнее время мировые тенденции диктуют повсеместное использование облачных хранилищ для своих нужд: как корпоративных, так и личных. Но представители технической общественности стали чаще задаваться вопросом безопасности информации, хранящейся в этих самых «облаках».

Работу с информацией при хранении ее в «облаке» можно разделить на 3 этапа:

1) Подготовка информации к отправке. Осуществляется пользователем на личной/корпоративной рабочей машине.

2) Идентификация и аутентификация в облачном хранилище и передача файлов по каналу связи.

3) Хранение файлов в «облаке».

Безопасность информации, хранимой в «облаках», обеспечивается несколькими компонентами:

– безопасностью данных (предотвращение угроз техническими способами и методами);

– управлением идентификацией и доступом (регулирование доступа пользователей);

– административным контролем (политика предотвращения, обнаружения и устранения угроз);

– резервное копирование (создание мер восстановления утерянных данных в случае технического сбоя);

– соблюдением нормативно-правовых требований [3].

Каждый компонент обеспечения безопасности характерен для одного или нескольких этапов работы с информацией в «облаках». Так, резервное

копирование, безопасность данных и управление идентификацией и доступом осуществляют защиту на всех этапах. Такой компонент, как административный контроль, позволяет обеспечить защиту при подготовке к отправке и при хранении файлов в «облаке». Соблюдение нормативно-правовых требований обеспечивает защиту рабочей станции пользователя и канала связи.

Можно заметить, что единственным компонентом, который не позволяет обеспечить безопасность информации в облачных хранилищах, является соблюдение нормативно-правовых требований. Этот факт объясняется отсутствием в российском законодательстве нормативно-правовых документов, которые напрямую относились бы к этому вопросу.

В рамках данной исследовательской работы одним из вариантов защиты информации и повышения доверия к облачным системам хранения данных предлагается использование криптографических методов, алгоритмов и средств.

Прежде чем выбирать конкретные решения, необходимо было понять, для кого они будут предназначены. Так как для физических лиц и государственных информационных систем требования к средствам защиты отличаются. Для последних обязательным условием использования средства защиты является наличие у него сертификата соответствия требованиям ФСБ России [2].

К таким сертифицированным средствам можно отнести:

– КриптоПро CSP;
– JC-WebClient;
– ViPNet CSP [1, с.244].

Программные продукты, которые могут использовать физические лица для защиты своих данных, следующие:

– EncFS;
– TrueCrypt;
– Boxcryptor;
– Mega.

Другим вариантом обеспечения безопасности информации, хранящейся в облаке, является использование биометрической составляющей пользователя для входа в систему. Самым популярным компонентом считается отпечаток пальца. Чаще всего он применяется в мобильных телефонах при входе в приложение, также иногда в некоторых ноутбуках, оборудованных соответствующим считывателем.

Работа продолжится изучением защищенности средств виртуализации и разработкой подходов по повышению доверия к обеспечению информационной безопасности распределенных систем.

Примечание

[1] Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ) №26/2020.

Список литературы

1. К вопросу регулирования безопасности «облаков» / Корх И.А., Маврешко В.М. В сборнике: Перспектива-2019. Материалы VIII Всероссийской молодежной школы-семинара по проблемам информационной безопасности. 2019. С. 241–245.

2. Приказ ФСБ РФ от 13 ноября 1999 г. № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия».

3. Что такое безопасность облака? | Лаборатория Касперского [Электронный ресурс]: https://www.kaspersky.ru/resource-center/definitions/what-is-cloud-security (дата обращения: 12.10.2021)

ЧЕЛОВЕЧЕСКИЙ ФАКТОР И СОСТОЯНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ [1]

Корх Ирина Анатольевна
Старший преподаватель кафедры КТиИБ
Кубанский государственный технологический университет,
Московская ул., 2, 350072 г. Краснодар, Краснодарский край,
Российская Федерация
aia2004@inbox.ru
Юсупов Юсуп Анварович
Студент,
Кубанский государственный технологический университет,
Московская ул., 2, 350072 г. Краснодар, Краснодарский край,
Российская Федерация
Стоев Давид Андреевич,
Студент,
Кубанский государственный технологический университет,
Московская ул., 2, 350072 г. Краснодар, Краснодарский край,
Российская Федерация

Аннотация. В статье рассмотрены подходы для минимизации влияния человеческого фактора на защищенность информационных систем. Предложено в качестве основного метода воздействия повышать осведомленность сотрудников в вопросах информационной безопасности и проводить инструктажи на рабочем месте с учетом возможных атак социальной инженерии. Представлен прототип программного продукта для проведения инструктажей по информационной безопасности.

Ключевые слова: осведомленность, человеческий фактор, инструктаж, доверие к обеспечению информационной безопасности.

THE HUMAN FACTOR AND THE STATE OF SECURITY OF INFORMATION SYSTEMS IN THE DIGITAL ECONOMY [1]

Korkh Irina Anatolievna
Senior Lecturer
Kuban State Technological University,
Moskovskaja ul., 2, 350072 g. Krasnodar, Krasnodarskij kraj,
Russian Federation
aia2004@inbox.ru
Yusupov Yusup
Student
Kuban State Technological University,
Moskovskaja ul., 2, 350072 g. Krasnodar, Krasnodarskij kraj,
Russian Federation
Stoev David
Student
Kuban State Technological University,
Moskovskaja ul., 2, 350072 g. Krasnodar, Krasnodarskij kraj,
Russian Federation

Abstract. The article considers approaches to minimize the influence of the human factor on the security of information systems. It is proposed as the main method of influence to raise the awareness of employees in information security issues and conduct briefings at the workplace, taking into account possible attacks of social engineering. A prototype of a software product for conducting information security briefings is presented.

Key words: awareness, human factor, instruction, trust in information security.

Основной целью исследования является повышение уровня осведомленности сотрудников в вопросах информационной безопасности (ИБ) с учетом возможных атак социальной инженерии [1]. Цель достигается за счет индивидуального подхода к проведению инструктажа и

автоматизации процесса обучения путем использования экспертных правил, и методов машинного обучения.

В источниках и научных исследованиях существуют описания информационных и автоматизированных систем обработки персональных данных, подробно изучены угрозы и нарушители, составлены частные модели угроз. Техническое направление достаточно изучено, но по опыту работы, наибольшую угрозу представляют собственные сотрудники вне зависимости от мотива действий. Практическая новизна исследования заключается в автоматизации инструктажа на рабочем месте, проводимого сотрудником службы информационной безопасности в соответствии с лицензионными требованиями в части исполнения функций органа криптографической защиты (может применяться в банковской, налоговой и иной деятельности, а также в удостоверяющем центре, содержащем большое число сотрудников, допущенных к работе со средствами криптографической защиты). Инструктаж должен проводиться с учетом возможной уязвимости сотрудников к методам социальной инженерии, потому представляется обоснованным проведение вводного тестирования для определения психологических особенностей личности сотрудника.

Предложенное решение не содержит баз данных переписки сотрудников и не может рассматриваться как психолингвистический анализ, не относится к DLP-системам. Научная новизна заключается в использовании для анализа данных и формирования текста инструктажа персонификации, проводимой методами искусственного интеллекта.

В работе предлагается применение методики «7 радикалов» В.В. Пономаренко [2]. Выбор обусловлен необходимостью дальнейшей автоматизации и внедрения в организацию, что не позволило применять в полной мере метод А.Е. Личко и Е. Леонгарда. В психологии, для определения сильных и слабых сторон личности используют совмещенный опросник Леонгарда-Шмишека. Применение его для целей информационной безопасности также затруднено.

Использование методики «7 радикалов» в информационной безопасности не является новизной. Она внедрена в некоторые DLP-системы, оснащенные модулями психолингвистики [3]. Однако, в данной работе такой подход без модификации не приемлем, поскольку критериями определения ведущего радикала являются:

– внешность (нельзя использовать для автоматизации анализ жестов, походки, мимики);

– особенности поведения (привычки требуют длительного изучения, что не соответствует целям, поставленным в работе);

– оформление пространства (нет возможности использовать знания, поскольку инструктаж проводится для вновь набираемых сотрудников и нет сведений об их предпочтениях в организации рабочего места).

Модель доступа к опроснику со стороны тестируемого представлена на рисунке 1. В программном продукте предусмотрено три роли: тестируемый, администратор и сотрудник отдела кадров. При необходимости проведения инструктажа по лицензируемой деятельности, роль сотрудника отдела кадров выполняется специалистом по информационной безопасности органа криптографической защиты.

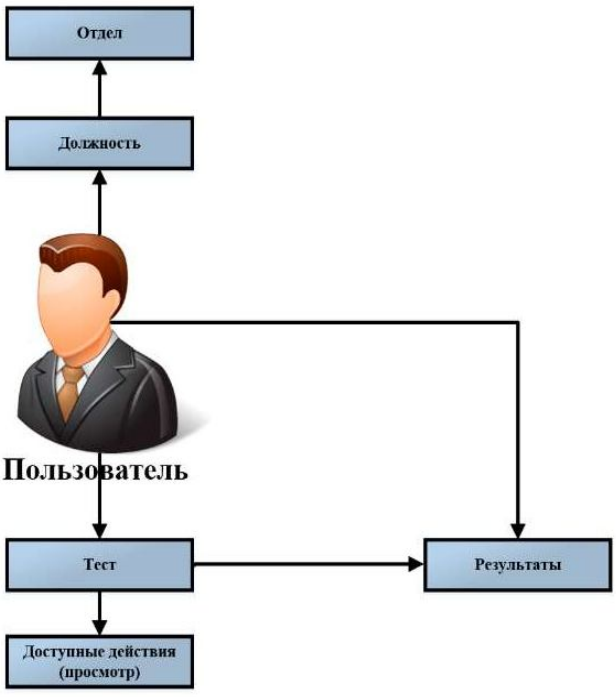

Рис. 1. Модель доступа

Схема реализации программного продукта представлена на рисунке 2. Для реализации выбран язык программирования Python, поскольку он позволяет работать с нейронными сетями и использовать в качестве платформы операционные системы нескольких семейств.

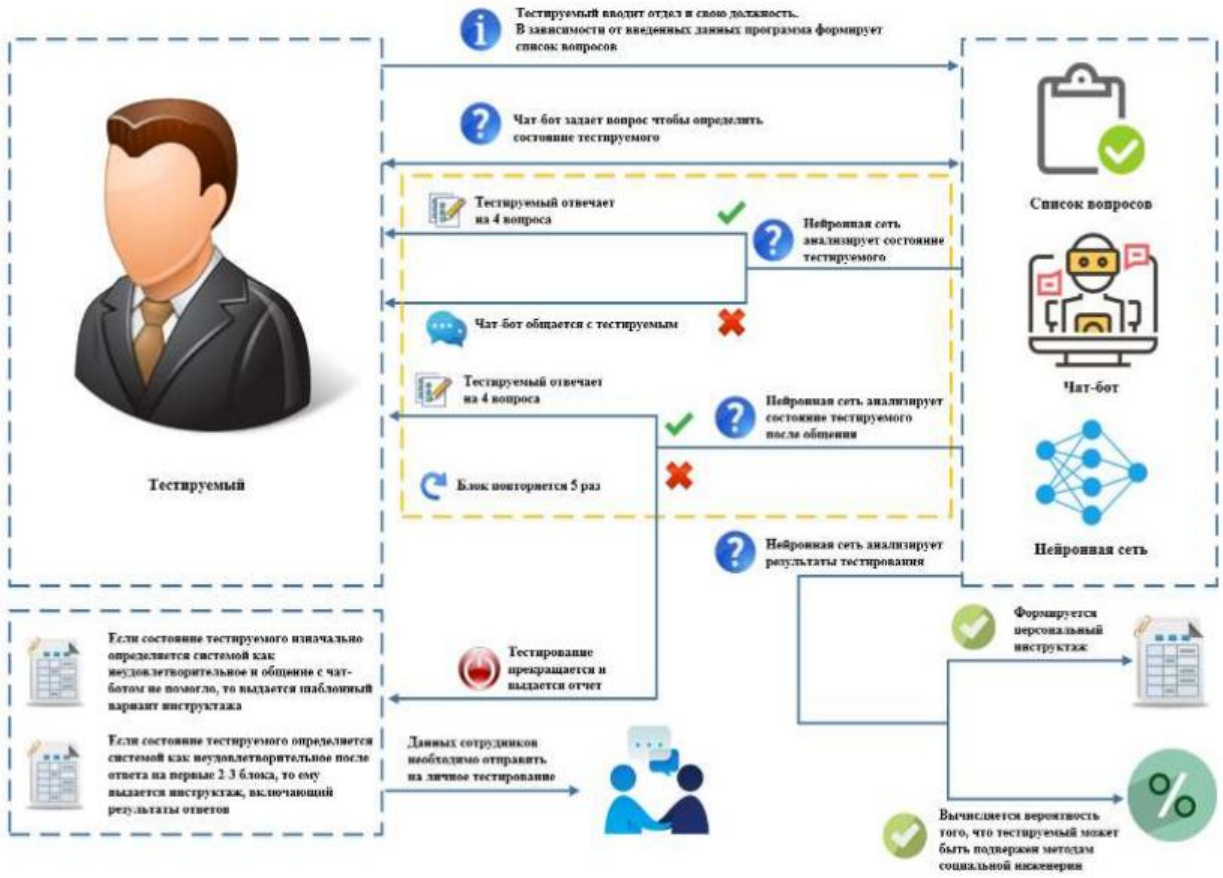

Рис. 2. Схема реализации программного продукта

На данный момент проводятся работы по тестированию разработанного программного продукта на реальных испытуемых. Далее планируется определение погрешности эксперимента и точности разработанной методики.

Примечание

[1] Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ) №26/2020

Список литературы

1. Чернецова Т.В., Корх И.А., Зангиев Т.Т. Атака на человека // Социотехнические и гуманитарные аспекты информационной

безопасности». Материалы II Всероссийской научно-практической конференции. Пятигорск: ПГУ, 2020. – 160-165.

2. Практическая характерология: методика 7 радикалов / В.В. Пономаренко. – Москва : Издательство АСТ, 2019. – 224 с. – (Практический тренинг).

3. Принцип работы DLP-системы [Электронный ресурс]: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/printsip-raboty-dlp-sistemy/ (дата обращения 28.09.2021).

ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ ЭЛЕМЕНТОВ АВТОМАТИЗИРОВАННОЙ БАНКОВСКОЙ СИСТЕМЫ

Медведев Артур Романович
студент кафедры информационной безопасности
Волгоградского государственного университета
ibb-181_215135@volsu.ru
Проспект Университетский, 100, 400062 г. Волгоград, Российская Федерация
Омельченко Татьяна Александровна
старший преподаватель кафедры информационной безопасности
Волгоградского государственного университета
omelchenko.tatiana@volsu.ru
Проспект Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Статья посвящена вопросам особенностей обеспечения безопасности автоматизированной банковской системы. Рассматриваются основные уязвимости, которым она подвержена, их виды в зависимости от источника происхождения угрозы, механизмы обеспечения защиты и противодействия некоторым видам атак.

Ключевые слова: Автоматизированная банковская система, информационная безопасность, уязвимости, угрозы, противодействие атакам на элементы автоматизированных банковских систем

INVESTIGATION OF THE SECURITY OF AN AUTOMATED BANKING SYSTEM ELEMENTS

Medvedev Artur Romanovich
Student of department of Information Security,
Volgograd State University
ibb-181_215135@volsu.ru
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation.
Omelchenko Tatiana Aleksandrovna
senior lecturer of department of Information Security,
Volgograd State University
omelchenko.tatiana@volsu.ru
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation.

Abstract. The article is devoted to the issues of security features of the automated banking system. The main vulnerabilities to which it is exposed, their types depending on the source of the threat, mechanisms for ensuring protection and countering certain types of attacks are considered.

Key words: Automated banking system, information security, vulnerabilities, threats, countering attacks on elements of automated banking systems.

На всех этапах человеческого развития информация являлась обособленным от других материальных благ ресурсом, но это не мешало ей оставаться одним из ключевых источников успешного достижения целей, поставленных в различных сферах. На сегодняшний день ценность обладания различными сведениями растет экспоненциально с каждым днем. Такая острая потребность в данных привела к появлению отдельного криминального сектора-цифрового. Теневые организации и различные хакерские группировки ежедневно осуществляют десятки тысяч различных атак на многие государственные и частные структуры. Некоторые из них удается отразить, но немалый процент кибернападений является успешным. Подобная ситуация навязывает обществу необходимость в массовом

создании и внедрении в эксплуатацию различных сетевых устройств, предназначение которых сводится к мониторингу событий, происходящих внутри локальной сети, а также, в случае выявления угрозы, всяческое препятствование проникновению злоумышленников в киберпространство предприятия.

Являясь немаловажной частью повседневной жизни, банковский сектор также подвержен всем проблемам информационной безопасности, описанным выше.

Рассмотрим типовую структуру автоматизированной банковской систему, представленную на рисунке 1.

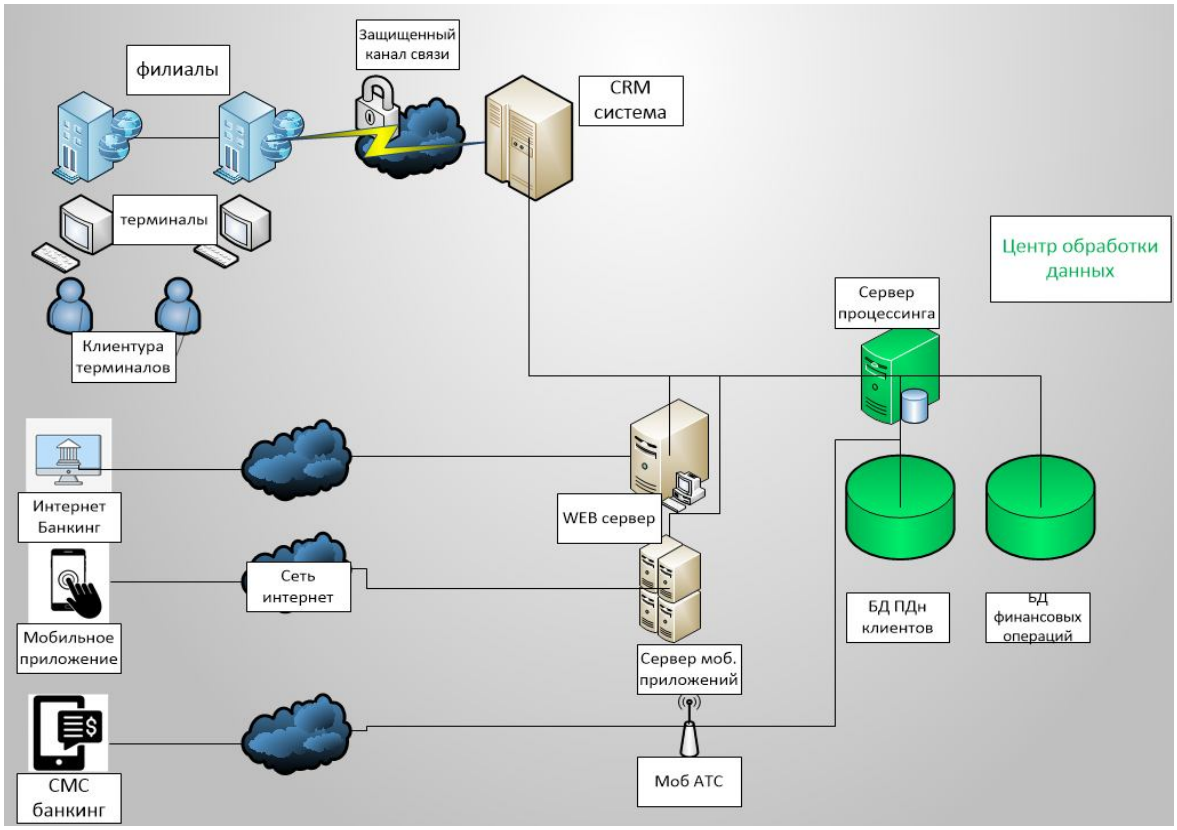

Рис. 1. Типовая структура автоматизированной банковской системы

Анализируя схему, продвигаясь от левой части к правой, можно выделить архитектурные уровни автоматизированной банковской системы, для дальнейшего их разбора на предмет уязвимостей и угроз.

Уровень пользователя (клиентский уровень) – представляет собой совокупность клиентов банка, осуществляющих использованние ДБО.

Уровень ввода учетных данных на устройствах ввода – вывода ДБО – является первой ступенью взаимодействия клиента и абс: включает в себя различные варианты подключения (представлены на схеме)

Уровень передачи информации по каналу связи – является промежуточным уровнем, соединяющим отдельные компонеты АБС, включает в себя сетевые устройства, соединительные кабели и пр.

Уровень веб-серверов – представляет собой сервер, осуществляющий взаимодействие с клиентами, по протоколу HTTP и другим сопутствующим веб-технологиям.

Уровень баз данных (БД) – включает в себя сервер БД обслуживающий и управляющий базами данных. Основными функциями, возлагаемыми на сервер БД являются обеспечение целостности и сохранности данных, а также осуществление операций ввода-вывода при доступе клиента к информации.

Для определения целесообразности применения тех или иных механизмов и средств обеспечения безопасности компонентов автоматизированной банковской системы (АБС), необходимо выявить типы персональных данных (ПДн) циркулирующих внутри данной ИСПДн. Помощником в этом будет служить Политика обработки персональных данных в ПАО Сбербанк, а также иные руководящие документы и законодательные акты. Выделяют следующие две категории персональных данных, обрабатываемых АБС. К первой относят общедоступные, т.е. любую информацию, относящуюся к субъекту персональных данных, обрабатываемую Банком для достижения заранее определенных целей. Ко второй относят специальные, в том числе данные, касающиеся состояния здоровья субъекта персональных данных. Банк вправе осуществлять обработку биометрических персональных данных с целью идентификации клиентов и работников Банка, при оказании банковских услуг и установления личности работников и посетителей при осуществлении пропуска на территорию Банка.

Для выяснения типов субъектов ПДн, контактирующих со службами банка в целом и с АБС в частности, а, следовательно, целесообразности внедрения конкретного типа оборудования и (или) средств защиты информации (СРЗИ) обратимся к тому же самому документу.

Банк осуществляет обработку персональных данных семи категорий Субъектов ПДн, а именно, физических лиц если они: являются представителями Корпоративного клиента, кандидатами, работниками Банка и их близкими родственниками или розничными клиентами Банка; выполняют работы по оказанию услуг и заключили с Банком договор гражданско-правового характера; входят в органы управления Банка; приобрели или намереваются приобрести услуги Банка, услуги третьих лиц при посредничестве Банка или не имеют с Банком договорных отношений при условии, что их персональные данные включены в автоматизированные системы Банка и обрабатываются в соответствии с Законодательством о персональных данных.

Полагаясь на Постановление Правительства № 1119 от 1 ноября 2012, определим уровень защищенности рассматриваемой типовой АБС (рисунок 2).

Категории ПДн		Специальные			Биомет-рические	Иные			Общедоступные		
Собственные работники		нет	нет	да		нет	нет	да	нет	нет	да
Количество субъектов		более 100 тыс.	менее 100 тыс.			более 100 тыс.	менее 100 тыс.		более 100 тыс.	менее 100 тыс.	
Тип актуальных угроз	1	1 УЗ	1 УЗ	1 УЗ	1 УЗ	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ
	2	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	3 УЗ	3 УЗ	2 УЗ	3 УЗ	3 УЗ
	3	2 УЗ	3 УЗ	3 УЗ	3 УЗ	3 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ

Рис. 2. Определение уровня защищенности АБС

Проанализировав категории ПДн, количество субъектов, а также тип актуальных угроз, делаем вывод о том, что данная ИСПДн (АБС) должна соответствовать второму уровню защищенности. Поэтому необходимо применять технические меры по защите информации для данного уровня

защищенности в соответствие и во исполнение действующих законодательных актов.

Список литературы

1. Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации/ Общие положения»

2. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»

3. Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения»

4. ГОСТ Р ИСО/МЭК 15408-1-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»

5. ГОСТ Р ИСО/МЭК 15408-2-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности»

6. ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности»

ЗАЩИЩЕННАЯ СИСТЕМА УПРАВЛЕНИЯ СОДЕРЖИМЫМ WEB-РЕСУРСА

Никишова Арина Валерьевна

кандидат технических наук,

доцент кафедры информационной безопасности

Волгоградского государственного университета

nikishova.arina@volsu.ru

Проспект Университетский, 100, 400062 г. Волгоград, Российская Федерация

Умницын Михаил Юрьевич
кандидат технических наук,
доцент кафедры информационной безопасности
Волгоградского государственного университета
umnitsyn@volsu.ru
Проспект Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В современных условиях, когда все больше взаимодействий с окружающим миром переходит в дистанционный режим, безопасность WEB-ресурсов имеет большое значение. По результатам анализа прогнозируемых актуальных уязвимостей WEB-ресурсов, предложена архитектура защищенной системы управления содержимым WEB- ресурса.

Ключевые слова: WEB-ресурс, управление информационным наполнением, уязвимость, модуль защиты, защищенная система.

SECURE CONTENT MANAGEMENT SYSTEM OF WEB RESOURCE

Nikishova Arina Valerevna
Candidate of technical sciences
Associate professor of Department of information security,
Volgograd State University
nikishova.arina@volsu.ru
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation
Umnitsyn Mikhail Yurievich
Candidate of technical sciences
Associate professor of Department of information security,
Volgograd State University
umnitsyn@volsu.ru
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation

Abstract. In modern conditions, when more and more interactions with the outside world are moving into remote mode, the security of WEB resources is of

great importance. Based on the results of the analysis of the predicted vulnerabilities of WEB resources, the architecture of the secure content management system of a WEB resource is proposed.

Key words: WEB resource, content management system, vulnerability, security unit, secure system.

Управление информационным наполнением WEB-ресурсов широко распространено в виде CMS-средств на рынке программного обеспечения. [1] Это обусловлено тем, что поддержание содержимого WEB-ресурсов в актуальном состоянии, так же как и управление всеми данными, принадлежащими организации, определяет успешность компании. Обычно от CMS-средства требуется наличие такого функционала как обеспечение централизации управления хранящимися данными, разделение содержания данных и их представления, автоматизация функций документооборота организации в части этапа наполнения системы данными, поддержание совместного обращения различных пользователей к одним и тем же данным, предоставление пользователям доступа к данным различными способами [2].

Прогнозы, даваемые для уязвимостей WEB-ресурсов в 2021 году, включают следующие уязвимости:

— инъекции. При этом наиболее часто по-прежнему встречаются SQL-инъекции;

— недостатки системы аутентификации. Основными причинами возникновения таких проблем являются нестойкость пароля, а также несвоевременное его обновление и незащищенность хранения;

— раскрытие конфиденциальных данных. За последние несколько лет количество утечек значительно увеличилось. К этому приводит недостаточная защищенность хранимых данных;

— небезопасная конфигурация. Эта уязвимость кроется в использовании небезопасных настроек по умолчанию или устаревших компонентов;

— XSS – межсайтовый скриптинг. Несмотря на то, что не все виды WEB-ресурсов подвержены данной уязвимости в связи с особенностями ее реализации, она представляет большую угрозу, от которой необходимо предусмотреть защиту;

— небезопасная десериализация. Это новая угроза, которая возникает, если принимать сериализованные объекты из вредоносных или ненадежных источников;

— использование компонентов с известными уязвимостями. Если несвоевременно обновлять версии таких компонентов, как библиотеки или фреймворки, то весь ресурс будет под угрозой;

— недостатки журналирования и мониторинга. Последствия реализации многих угроз можно предотвратить, если вовремя заметить проблему и устранить ее. Однако это требует журналировать и анализировать данные о текущем состоянии WEB-ресурса в полном объеме;

— SMS-флуд. Аналог DoS-атак для тех WEB-ресурсов, которые используют дополнительные подтверждения через SMS-сообщения.

Для того чтобы повысить защищенность WEB-ресурса предлагается дополнить архитектуру системы управления содержимым Web-ресурса [3] несколькими модулями (рисунок 1).

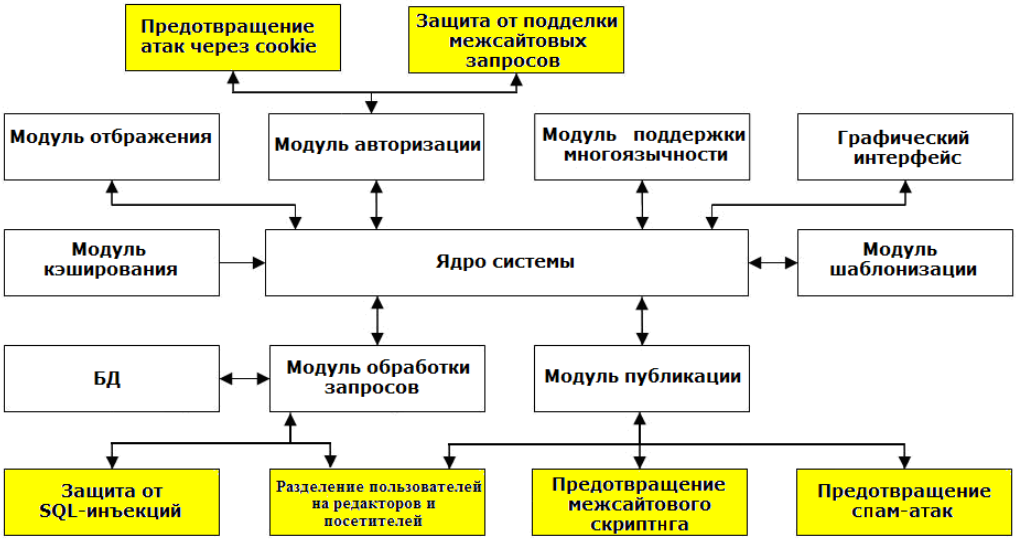

Рис. 1. Архитектура защищенной системы управления содержимым WEB-ресурса

Дополнив систему управления содержимым WEB-ресурса модулем предотвращения атак через cookies, модулем защиты от подделки межсайтовых запросов, модулем защиты от SQL-инъекций, модулем разделения пользователей на роли, модулем предотвращения межсайтового скриптинга и модулем предотвращения спам-атак, можно снизить риски нарушения конфиденциальности и целостности WEB-ресурса, а также повысить его доступность.

Список литературы

1. Герасимова А.В. CMS технологии как современное средство для создания веб-сайта // Наука, образование и культура. 2019. №6 (40).

2. Кухаренко В. Основные тренды веб-разработки 2021. На какие тенденции нужно обратить внимание? // Системный администратор. 2021. №3 (220). С. 18–22.

3. Алексеев А.А. Способы и методика написания WEB-сайтов // сборник статей XXV Международной научно-практической конференции European scientific conference. Пенза, 2021. С. 20–23

ОСОБЕННОСТИ ЭКОНОМИЧЕСКОГО ОБОСНОВАНИЯ ЗАТРАТ НА ПРОЕКТЫ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ

Петрищева Татьяна Сергеевна

Кандидат экономических наук,

доцент кафедры информационной безопасности

Института приоритетных технологий ВолГУ

Ts_pet@mail.ru

Проспект Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В статье рассмотрены некоторые вопросы экономического обоснования затрат на проекты по информационной безопасности в условиях цифровой экономики. Приведены примеры взаимосвязи информационных проектов с бизнес-проектами. Обоснована необходимость

серьезных изменений функций специалистов по безопасности в связи со все большей цифровизацией современной экономики.

Ключевые слова: цифровая экономика, информационная безопасность, затраты на проекты по информационной безопасности, специалист по безопасности, информационные проекты.

FEATURES OF THE ECONOMIC JUSTIFICATION OF THE COSTS OF INFORMATION SECURITY PROJECTS IN THE CONDITIONS OF DIGITALIZATION OF THE ECONOMY

Petrishcheva Tatiana Sergeevna
Candidate of Economic Sciences
Associate Professor of the Department of Information SecurityInstitute
of Priority Technologies of the Volga State University
Ts_pet@mail.ru
Prospekt Universitetskiy, 100, 400062 Volgograd, Russian Federation

Abstract. The article discusses some issues of economic justification of the costs of information security projects in the digital economy. Examples of the relationship of information projects with business projects are given. The necessity of serious changes in the functions of security specialists in connection with the increasing digitalization of the modern economy is substantiated.

Key words: digital economy, information security, costs of information security projects, security specialist, information projects.

Бурное развитие цифровой экономики в силу прорывных технологических разработок наряду с ростом уровня угроз создает более сложные экосистемы для компаний и их сотрудников, занимающихся вопросами безопасности. Требуются серьезные изменения функций специалистов по безопасности: такие как обоснование соответствия потребности в информационной безопасности бизнес-целям компании. Хотя профиль руководителей по информационной безопасности все еще остается

техническим, его связь с бизнес-целями требует определенных способностей и более широкого видения бизнеса. Этим обусловлена актуальность данного исследования.

Обычно в коммерческой организации информационная безопасность (ИБ) рассматривается как часть большого бизнес-проекта. Надо понимать, насколько важен бизнесу данный проект и важность ИБ в нем, что бы обосновать необходимость финансовых затрат на ИБ в проекте. То есть важно обосновать затраты на ИБ с точки зрения бизнеса, а не с точки зрения самой безопасности. Например, задача компании – изменить стратегию продаж с целю увеличения выручки от реализации. За счет чего можно увеличить выручку? Это можно сделать за счет роста числа клиентов и сделок, ускорение сделок, за счет снижения себестоимости. Рост числа клиентов может быть достигнут, например, за счет открытия новых офисов, что бывает не всегда целесообразно и экономически оправдано. А можно без открытия офисов привлечь работников, предоставив им защищенный доступ к ИС компании, чтобы они ездили к клиентам и заключали договора на месте. Соответственно, географическая экспансии компании на рынке осуществляется несколькими отделами, в том числе и ИБ, которые организуют защищенный доступ к ИС компании.

Рост числа сделок может быть достигнут путем «выноса» точки продаж в «поле». Например, многие банки открывают небольшие офисы в торговых центрах. Это устраивает всех участников рыночных отношений: клиента, так как ему не нужно ехать в офис банка для оформления кредита, ТЦ увеличивает выручку, за счет большей покупательной способности покупателей, благодаря кредиту, а банк увеличивает клиентскую базу. Так же упрощается сама сделка и увеличивается ее скорость. Вынос точки продаж «в поле» приводит к тому, что работникам необходим защищенный доступ (стационарный или мобильный). Таким образом, ИБ здесь выступает, как часть большого проекта, приносящего очевидные выгоды компании.

Ускорение сделок очень наглядно можно показать на примере интернет-магазинов и интернет-банков, которые в последнее время очень активно развиваются. Благодаря такой организации бизнеса, решается задача сокращения себестоимости: интернет-магазин практически не имеет сотрудников, охранников, офиса. Этот проект всегда требует информационной защиты.

Одной из целей компании может быть снижение себестоимости за счет арендной платы. Понятно, что безопасность напрямую не приводит к снижению арендной платы. Однако, если необходимо перенести офис в другое место, где арендная плата меньше, а это требует времени, затрат, перевода сотрудников, то задачу можно решить иным путем: перевести часть сотрудников компании на надомную работу. В этом случае возникает комплексный проект по защищенному надомному доступу. При этом, компания экономит за счет арендных платежей, затрат на коммунальные услуги, оплата проездных сотрудникам, роста производительности труда сотрудников. Рост производительности возникает благодаря уменьшению времени, которое потрачено на дорогу до работы, стояние в пробках и т.д.

Интересный пример приводит Алексей Лукацкий – бизнес-консультант по вопросам информационной безопасности компании Cisco (телекоммуникационная компания, занимающаяся производством сетевого оборудования) [1]. В данной компании были уменьшены складские площади, наличие которых требовало больших затрат и которые не всегда эффективно эксплуатировались. Проведена оптимизация следующим образом: был предоставлен удаленный доступ к отдельным частям складской системы компании поставщику, таким образом, поставщик самостоятельно мог отслеживать нехватку тех или иных материалов и, по необходимости, обеспечивать их доставку. Соответственно, доступ через интернет к складской ИС был защищен. Благодаря произведенной оптимизации компания Cisco в 1,5 раза сократила складские площади, за которые теперь не нужно платить.

Таким образом, когда мы говорим о затратах на ИБ, важно отметить и отдачу от внедренных ИБ-проектов. О каких выгодах мы можем говорить в контексте информационной безопасности с точки зрения бизнеса? В частности – это получение доходов, снижение расходов или потерь, снижение времени на какие-либо операции, высвобождение трудовых ресурсов и более эффективное использование труда.

В конце, хотелось бы отметить, что в некоторых зарубежных компаниях, понимая значительную роль ИБ в бизнес-проектах, вводят в штат должность «директор по информационной безопасности» (CISO, Chief Information Security Officer) [2]. Хотя профиль руководителей по ИБ технический, его связь с бизнес-целями требует определенных способностей и более широкого видения бизнеса. Думается, что данное утверждение коснется будущих специалистов по ИБ в целом. Так, согласно исследованию Ponemon Institute, 67% руководителей ИБ ответственны за разработку и внедрение стратегий и инициатив по безопасности своих компаний. 69% респондентов в исследовании Ponemon считают, что назначение директора по безопасности с корпоративной ответственностью является фундаментальным моментом для компании. CISO будущего должен отчитываться о своей деятельности внутри организации, рассчитывать бюджет, а также реализовывать бизнес-тактики в соответствии с целями предприятия [2].

Вывод. В условиях цифровой экономики специалист по безопасности должен работать в соответствии с потребностями предприятия. Хотя за данными специалистами остается ответственность за обеспечение постоянной работы ИТ-сервисов и соответствие всем законодательным требованиям, они должны будут уметь обосновывать финансовые затраты на это обеспечение.

Список литературы

1. А. Лукацкий. Совершенствование защиты на всех уровнях [Электронный ресурс]. – Режим доступа https://www.vedomosti.ru/forum/

technologii_novoj_realnosti/columns/2020/12/02/849239-sovershenstvovanie-zaschiti (дата обращения 25.10.2021).

2. Директор по информационной безопасности [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/Статья:Директор_по_информационной_безопасности_(Chief_information_security_officer,_CISO) (дата обращения 25.10.2021).

СРАВНЕНИЕ SIEM СИСТЕМ

Пономарев Михаил Витальевич

Студент кафедры информационной безопасности,

Волгоградский государственный университет

просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В данной статье был проведен анализ существующих SIEM систем. Приводится статистика распределения утечек информации. Описываются принципы работы SIEM систем.

Ключевые слова: SIEM система, внешний нарушитель, внутренний нарушитель, информационная безопасность, журналы безопасности, инциденты безопасности.

COMPARISON OF SIEM SYSTEMS

Ponomarev Mikhail Vitalievich

Student of Department of Information Security,

Volgograd State University

Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation

Abstract. In this article, an analysis of existing SIEM systems was carried out. The statistics of the distribution of information leaks is given. The principles of operation of SIEM systems are described.

Key words: SIEM system, external intruder, insider, information security, security logs, security objects.

Согласно недавнему отчету экспертно-аналитического центра InfoWatch [1] основной вектор атак за последние годы все больше смещается в сторону внешнего нарушителя. Действия хакеров и неизвестных лиц из-за пределов информационного контура организаций в 2020 году привели к 55,9% утечек (рисунок 1).

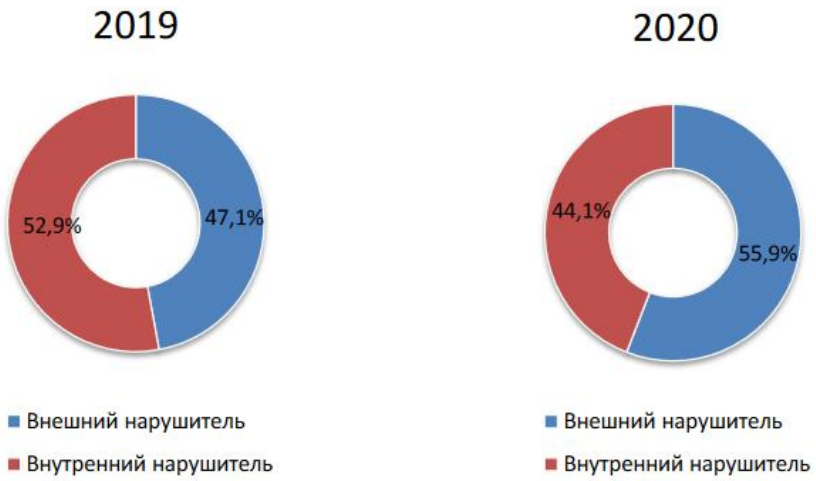

Рис. 1. Распределение утечек по вектору воздействия, 2019–2020 гг.

На фоне пандемии и массового перехода на удаленную работу стало намного больше уязвимых точек в системе безопасности организаций эксплуатируемых злоумышленниками. В связи с этим наиболее актуальным становится усиление системы мониторинга инцидентов безопасности на территории организации.

SIEM (Security information and event management) – обеспечивает анализ событий безопасности системы с помощью приложений и сетевого оборудования в режиме реального времени. Он включает в себя такие подсистемы, как мониторинг системы, анализ журналов, корреляция событий безопасности, реагирование на инциденты и т.д.

SIEM системы базируются на следующих принципах работы:

1. Анализ журналов безопасности.

2. Нормализация собранной информации в стандартный формат.

3. Уведомления и предупреждения – уведомление пользователя о возможных угрозах безопасности.

4. Обнаружение инцидентов безопасности.

5. Реагирования на угрозы.

SIEM анализирует данные внутренней сети и программных обеспечений пользователя и выявляет потенциальные проблемы и атаки. Система работает в рамках статистической модели для анализа записей журнала. SIEM распространяет агентов сбора и собирает данные из сети, устройств, серверов и межсетевых экранов, затем вся эта информация передается в консоль управления, где ее можно проанализировать для устранения возникающих угроз. Как только необходимая информация достигает консоли управления, она просматривается аналитиком данных, который может предоставить обратную связь по всему процессу. Как только программная система SIEM обнаруживает угрозу, она связывается с другими системами безопасности на устройствах, чтобы остановить нежелательную активность.

В таблице 1 приведено сравнение существующих решений SIEMсистем:

	Adlumin	Datadog	IBM QRadar	LogRhythm	OSSEC	Securonix	Splunk
Платформа	Windows	Облачная	RedHatEnterpriseLinux	Windows и Linux	Windows, Linux, Unix и Mac	Windows	Windows и Linux
Поддержка облачной технологии	Да	Да	Нет	Нет	Нет	Да	Нет
Интегрированная платформа анализа угроз	Да	Да	Да	Нет	Нет	Нет	Нет
Обнаружение угроз в реальном времени	Да	Да	Да	Да	Нет	Да	Нет
Адаптивные самообучающиеся модули	Да	Да	Да	Да	Нет	Да	Да

Обширная встроенная отчетность о соответствии (PCI DSS, NIST, HIPAA, ISO 270001, GLBA, FFIEC CAT, NCUA ACET и т. Д.)	Да	Нет	Нет	Нет	Нет	Да	Нет
Наличие шаблонов	Нет	Нет	Нет	Да	Да	Нет	Нет

По результатам анализа невозможно определить лучшую SIEMсистему, так что на сегодняшний день существует потребность в разработке собственных модулей безопасности, дополняющих функционал существующих SIEMсистем. Лучший способ интегрировать платформу SIEM в среду организации – вводить ее постепенно, настраивая под нужды конкретной организации, но при этом, не забывая совмещать как функции мониторинга в реальном времени, так и функции анализа журналов.

Список литературы

1. InfoWatch – Исследование утечек информации ограниченного доступа в 2020 году.

2. Check Point Research – Cybersecurity report – 2021.

3. Gustavo Gonzlez-Granadillo, Susana González-Zarzosa Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures - Cybersecurity Unit, Atos Research & Innovation, ATOS Spain, 28037 Madrid, Spain – 2021.

4. Хлестова Дарья Робертовна, Попов Кирилл Геннадьевич Анализ актуальности использования siem-систем на предприятиях // Символ науки. 2016. №7-1.

АНАЛИЗ МЕТОДОВ ОБНАРУЖЕНИЯ DDOS-АТАК

Попов Глеб Александрович
Старший преподаватель кафедры информационной безопасности,
Волгоградский государственный университет
gpopov@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация
Петренко Сергей Владимирович
Студент кафедры информационной безопасности,
Волгоградский государственный университет
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В данной статье был проведен анализ понятия DDOS-АТАК. Произведен анализ методов обнаружения DDOS-АТАК. Описываются основные свойства каждого метода и существующие подтипы методов.

Ключевые слова: DDoS-атака, трафик, информационная безопасность, защита данных

ANALYSIS OF DDOS ATTACK DETECTION METHODS

Popov Gleb Alexandrovich
Senior Lecturer of the Department of Information Security of
Volgograd state University
gpopov@volsu.ru
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation
Petrenko Sergey Vladimirovich
Student of Department of Information Security,
Volgograd State University
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation

Abstract. In this article, an analysis of the concept of DDOS ATTACKS was carried out. The analysis of methods for detecting DDOS-ATTACKS was carried out. The main properties of each method and the existing subtypes of methods are described.

Key words: DDoS attack, traffic, information security, data protection.

В современном мире возросла роль Интернета: электронные покупки и кошельки, трансграничные переводы, личная информация в социальных сетях и мессенджерах. Все это привело к появлению новых сетевых угроз, например, в последние три года среди хакеров стали популярны DDoS-атаки. Злоумышленники используют все более изощренные методы, старые средства перестают работать, требуются новые подходы и инструменты для того, чтобы не стать жертвой киберпреступников.

DDoS-атака (Distributed Denial of Service) – распределенная (идущая из разных источников) атака на интернет-ресурс с целью добиться его отказа, т.е. привести его в такое состояние, когда пользователи не могут получить к нему доступ. Часто злоумышленники генерируют большое количество пакетов или запросов, которые в итоге перегружают работу целевой системы. Для осуществления атаки типа «распределенный отказ в обслуживании» (DDoS) злоумышленник использует множество взломанных машин обычных пользователей.

Изучив существующие источники литературы [1-5] на данную тематику, можно прийти к выводу о множестве способов противодействия DDoS-атакам. По результатам анализа можно выделить три основных класса методов обнаружения DDoS-атак:

1. Статистические методы. Статистические свойства шаблонов DDoS атак могут быть использованы для их обнаружения. Тест на статистический вывод применяется для определения того, относится ли какой-либо новый экземпляр атаки к статистической модели обычного трафика. Экземпляры, которые не будут соответствовать изученной модели, классифицируются как аномалии. Самой известной схемой защиты от DDoS атак основанной на статистическом методе является D-WARD. Маршрутизатор с установленной системой D-WARD, которая действует как шлюз между исходной сетью и Интернетом, реализует непрерывное наблюдение за двусторонним трафиком. D-WARD периодически сравнивает собранную статистику с предопределенной моделью допустимого трафика, если результат сравнения

покажет, что существует вероятность DDoS-атаки, D-WARD установит ограничение скорости подозрительного исходящего потока для этого однорангового узла. Каждая запись потока, хранящаяся в D-WARD, содержит статистику по трем типам трафика: TCP, UDP и ICMP. Этот метод обеспечивает приличную скорость обнаружения, а также значительно снижает трафик DDoS-атак.

2. Методы, основанные на знаниях. В этом типе методов события атаки проверяются на соответствие предопределенным шаблонам атаки. Общие характеристики известных атак сформулированы таким образом, чтобы идентифицировать фактические случаи атак. Примеры этих подходов включают экспертные системы, самоорганизующиеся карты, анализ сигнатур и анализ перехода состояний.

На данный момент существует несколько технологий обнаружения DDOSатак, основанных на знаниях:

– MULTOPS – отслеживает определенные характеристики трафика, используемые маршрутизаторами для обнаружения и устранения DDoS-атак. Это дерево узлов, которое содержит статистику скорости передачи пакетов для префиксов подсети на разных уровнях агрегации.

– Фильтрация DDoS на основе легитимности клиента, известная как NetBouncer. Устройство NetBouncer поддерживает большой список легитимных клиентов, которые были признаны разрешенными. Если пакеты получены от клиента (источника), не включенного в список легитимности, устройство NetBouncer запустит тестирование клиента и в случае, если клиент может пройти эти тесты, он добавляется в список легитимности.

– Алгоритм обнаружения атак на основе AAT. Эта модель фиксирует шаблоны атак и соответствующие переходы состояний на основном сервере-жертве.

– Распределенный подход для обнаружения DDoS-атак. Этот подход самостоятельно обнаруживает и останавливает DDoS-атаки в промежуточной сети. Механизм связи используется для обмена данными о сетевых атаках

между независимыми узлами обнаружения для объединения данных об общих сетевых атаках. Отдельные узлы защиты получают приблизительные данные о глобальных сетевых атаках и могут предотвращать их более эффективно и точно.

3. Методы мягких вычислений. Компьютерные вычисления – это общий термин для описания набора методов оптимизации и обработки, которые допускают неточность и неопределенность.

Технологии относящиеся к методу мягких вычислений:

– SPUNNID, система обнаружения DDoS-атак, основанная на статистическом предварительном процессоре и неконтролируемых искусственных нейронных сетях. Методы статистической предварительной обработки используются для извлечения функций из трафика, а неконтролируемая нейронная сеть используется для исследования и классификации моделей трафика как DDoS-атаки, так и обычной.

– Метод обнаружения DDoS-атак на основе аномалий. Пакеты атак анализируются с использованием нейронных сетей с радиальной базисной функцией (RBF). Метод может быть применен к пограничным маршрутизаторам сетей-жертв. Семь характерных векторов используются для активации нейронной сети RBF в каждом временном окне. Нейронная сеть RBF классифицирует данные как обычные или атакующие.

– С использованием серого реляционного анализа и деревьев решений. Они используют пятнадцать атрибутов, которые отслеживают скорость ввода/вывода пакетов/байтов, а также компилируют скорости флагов TCP, SYN и ACK для описания структуры трафика. Метод дерева решений применяет классификатор для обнаружения аномального транспортного потока.

– Метод k-ближайшего соседа (KNN) для классификации состояния сети на каждом этапе DDoS-атака. Метод обнаруживает DDoS-атаки на основе нечеткой оценки с использованием среднего времени прибытия пакетов. Он обнаруживает подозрительный хост и отслеживает IP-адрес, чтобы отбросить пакеты в течение 3 секунд после обнаружения.

– В последнее время для обнаружения DDoS-атак используются ансамбли методов. Наибольшую эффективность показывают методы, основанные на нейросетевом анализе, где в качестве базового классификатора выбрана нейронная сеть с устойчивым обратным распространением (RBP).

В данной статье было рассмотрено несколько способов обнаружения DDoS-атак. В результате исследования было обнаружено, что в настоящее время все больше создаются и пользуются популярностью пользуются методы основанные на нейросетевом анализе.

Список литературы

1. Peng, T., Leckie, C., and Ramamohanarao, K. (2007) Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Survey, 39, 3:1–3:42.

2. Lin, S. and Chiueh, T. C. (2006) A survey on solutions to distributed denial of service attacks. Technical Report TR201, Department of Computer Science, State University of New York.

3. Chunming Zhang, "Impact of Defending Strategy Decision on DDoS Attack", Complexity, vol. 2021, Article ID 6694383, 11 pages, 2021.

4. L.-X. Yang, P. Li, X. Yang, Y. Xiang, F. Jiang, and W. Zhou, “Effective quarantine and recovery scheme against advanced persistent threat,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 1, 2020.

5. G. Liu, S. Peng, H. Qiu, B. Shi, and Y. W. Chen, “Voluntary vaccination through perceiving epidemic severity in social networks,” Complexity, vol. 2019, 2019.

МОДЕЛЬ ЗАЩИТЫ ОТ СПАМ-ФИШИНГА

Попова Александра Андреевна

студент кафедры информационной безопасности

Волгоградского государственного университета

IBS-171_256546@volsu.ru

Проспект Университетский, 100, 400062 г. Волгоград, Российская Федерация

Омельченко Татьяна Александровна
старший преподаватель кафедры информационной безопасности
Волгоградского государственного университета
omelchenko.tatiana@volsu.ru
Проспект Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В статье рассмотрены понятия спама и фишинговой атаки, описаны основные пути распространения атак данного вида. Предложена модель распознавания спам-фишинговых атак через электронную почту.

Ключевые слова: Информационная безопасность; спам; фишинг; электронная почта; атака; модель защиты.

SPAM PHISHING PROTECTION MODEL

Popova Alexandra Andreevna
Student of department of Information Security,
Volgograd State University
IBS-171_256546@volsu.ru
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation.
Omelchenko Tatiana Aleksandrovna
senior lecturer of department of Information Security,
Volgograd State University
omelchenko.tatiana@volsu.ru
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation.

Abstract. The article discusses the concepts of spam and phishing attacks, describes the main ways of spreading attacks of this type. A model for recognizing spam-phishing attacks via email is proposed.

Key words: Information Security; spam; phishing; Email; attack; protection model.

По данным инструментального анализа защищенности сетевых периметров корпоративных информационных систем positive technologies за

первую половину 2021 года в 84% организаций выявлены уязвимости высокого уровня риска и в 58% случаев данные уязвимости эксплуатируются через общедоступные эксплойты. На множестве ресурсов были обнаружены интерфейсы удаленного управления, предоставляющие внешним злоумышленникам возможность для реализации атак подбора учетных данных с дальнейшим подключением к атакованным сервисам. [1] Подбор простых паролей может занимать всего несколько минут, по истечению которых будет получен доступ к сетевому оборудованию с правами соответствующей учетной записи. Последствия таких действий могут нанести непоправимый вред атакованным ресурсам, и как следствие, их обладателям. Одним из векторов реализации подобных атак служит атака через электронную почту.

Использование небезопасных настроек почтового сервера, таких, как возможность выполнения команд VRFY, EXPN и RCPT TO позволяет злоумышленнику подбирать адреса электронной почты с возможностью автоматизации этого процесса через общедоступное программное обеспечение. Полученные таким образом адреса сотрудников в дальнейшем могут быть использованы при подборе учетных данных для подключения к различным сетевым ресурсам через службы удаленного доступа – либо для фишинговых рассылок (спама). [2]

Спам – это электронный заменитель бумажной рекламы, которую оставляют в почтовых ящиках. Однако, в отличии от обычных брошюр он становится источником опасности, если является частью фишинга. Жертва спам атаки не выбирается целенаправленно. Чаще всего фишинговые письма, распространяющиеся по сети, получают те, кто не заботится о своей безопасности или киберграмотности.

Фишинговые атаки реализуются через поддельную или мошенническую электронную почту. Направленные фишинговые атаки, нацелены на организации с высокой ценностью активов. Вместо того,

чтобы пытаться получить учетные данные каждого отдельного клиента одного банка, злоумышленник ориентируется сразу на несколько банков.

Во втором квартале 2021 года доступ к корпоративным аккаунтам по-прежнему оставался одной из самых заманчивых целей для злоумышленников. Чтобы пользователь больше доверял ссылкам в письме, мошенники имитировали рассылки от популярных облачных сервисов. Этот прием они и ранее неоднократно использовали. Поддельные уведомления о встрече в Microsoft Teams или просьбы посмотреть важный документ традиционно приводили жертву на странички с фишинговой формой для ввода логина и пароля от корпоративного аккаунта. После продолжительного снижения доля спама в мировом почтовом трафике снова начала расти и составила в среднем 46,56%. На данный момент наиболее актуальной рассылкой является информация о Covid-19, методы лечения и предложения приобрести сертификат вакцинации по привлекательной стоимости. [4]

Анализ представленных статистических данных позволяет сделать вывод о том, что проблема построения системы защиты от спам-фишинга на сегодняшний день остается актуальной, а следовательно, существует необходимость в разработке модели защиты от атак данного типа.

Реализация модели проверки письма на спам-фишинг, представлена в виде IDEF0-диаграммы (рисунок 1), и разделяется на несколько блоков: проверка адреса отправителя, анализ тела сообщения, распределение проверенных писем по папкам доступа.

В результате выполнения процесса, отправленное сообщение будет распределено по папкам в соответствии с положительной или отрицательной проверкой на спам-фишинг.

Процедуру распознавания спам-фишинг атак можно разделить на 3 основных этапа (таблица 1).

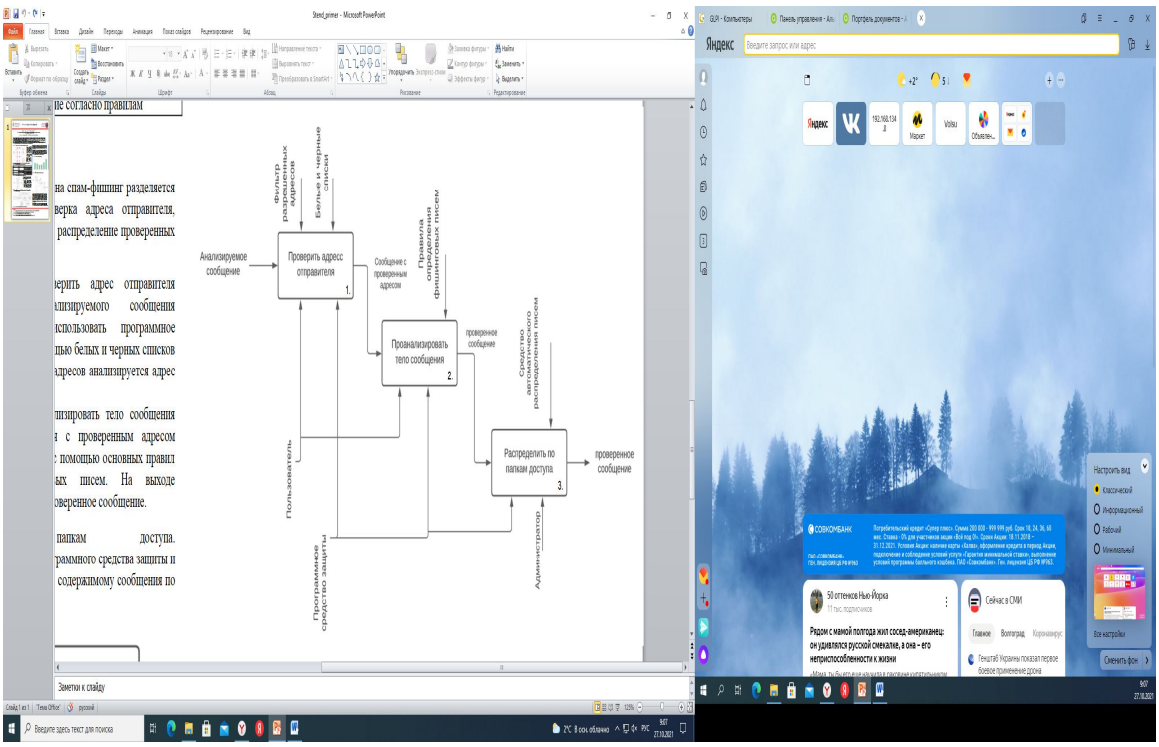

Рис. 1. IDEF0 диаграмма процесса защиты от спам-фишинга

Таблица 1

№	Этапы	Подэтапы	Описание этапов/подэтапов
1.	Загрузка входных данных	отсутствуют	Определение адреса входящего сообщения
			Загрузка адреса в обработчик
			Загрузка содержимого в обработчик
2.	Обработка входных данных	2.1 Проверка адреса отправителя	Выявление типа адреса
		2.2 Проверка тела сообщения	Определение безопасности содержимого
3.	Распределение	отсутствуют	Сопоставление в соответствии с правилами
			Распределение согласно правилам

Проверка адреса отправителя сообщения осуществляется в соответствии с белыми и черными списками адресов. Если адрес находится в черном списке, то сообщение автоматически помещается в спам. Если данный адрес не был найден в черном списке, то необходимо проверить тело сообщения на наличие фишинговых ссылок. Далее проводится проверка тела сообщение на наличие фишинговых ссылок. Если в сообщении были найдены ссылки или слова, которые помещены в список запрещенных, то данное сообщение помещается в спам, даже если оно было направлено от доверенного адреса. Если в сообщении не было найдено ссылок и слов, которые были помещены в список запрещенных, то данное сообщение помещается в общую папку. Помимо рассылок, так или иначе связанных с облачными сервисами, необходимо блокировать письма, замаскированные под деловую переписку и содержащие ссылки на вредоносное ПО.

Список литературы

1. Баранова Е., Бабаш А. Информационная безопасность и защита информации. Учебное пособие. 2019

2. Козлов С. Защита информации. Устройства несанкционированного съема информации и борьба с ними. Трикста, 2018, 289 с.

3. Магомедов Р.М. Анализ киберпреступности и борьба с ней // Экономика: вчера, сегодня, завтра. 2020. Том 10. № 6А. С. 48–54. DOI: 10.34670/AR.2020.30.24.006

4. Серия публикаций cisco по информационной безопасности, 2019 г. / Защита электронной почты, июнь 2019 г.

АНАЛИЗ МЕТОДОВ ОБФУСКАЦИИ

Попова Татьяна Александровна

Ассистент кафедры информационной безопасности,

Волгоградский государственный университет

popova.tatyana@volsu.ru

просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Крюченков Данила Алексеевич
Студент кафедры информационной безопасности,
Волгоградский государственный университет
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В данной статье был проведен анализ существующих методов обфускации исходного кода. Описываются основные свойства каждого метода и существующие подтипы методов.

Ключевые слова: Авторское право, обфускация, обратная разработка, информационная безопасность, защита данных

ANALYSIS OF OBFUSCATION METHODS

Popova Tatiana Aleksandrovna
assistant of the Department of Information Security of
Volgograd state University
popova.tatyana@volsu.ru
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation
Kryuchenkov Danila Alekseevich
Student of Department of Information Security,
Volgograd State University
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation

Abstract. In this article, an analysis of the existing methods of source code obfuscation was carried out. The main properties of each method and the existing subtypes of methods are described.

Key words: Copyright, obfuscation, reverse engineering, information security, data protection.

Авторское право – это юридический термин, используемый для описания прав авторов на результаты своей интеллектуальной или творческой деятельности. Работы, на которые распространяется авторское право, варьируются от книг, музыки, картин, скульптур и фильмов до компьютерных

программ и баз данных. Каждая организация сейчас имеет собственные разработки программного обеспечения и, следовательно, является актуальным вопрос защиты исходного кода программного кода этих программ.

С помощью методов обратной разработки злоумышленник может восстановить исходный код программного обеспечения и узнать принципы работы алгоритмов. На сегодняшний день самым доступным и действенным методом защиты исходного кода является обфускация.

Обфускация – это процесс запутывания исходного кода, т.е. приведение кода программы к виду, сохраняющему ее функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляции.

Существует несколько техник обфускациина уровне элементов кода:

1. Запутывание шаблона кода

– Обфускация имени – это процесс замены наименований элементов кода, таких как классы, методы, переменные и т.д. другими бессмысленными именами.

– Изменение порядка следования данных в программе – поменять расположение в коде переменных, функций и других логических частей, в том числе заменяя условные переходы на безусловные.

– Удаление избыточной информации – этот метод заключается в удалении избыточной информации из выпущенного программного обеспечения, такую как отладочная информация.

– Добавление нежелательного кода – это процесс добавления в код ненужных инструкций, которые не работают. Происходит увеличение кода за счет добавления частей кода, которые не влияют на результат работы исходного кода.

2. Запутывающие элементы управления

– Поддельные потоки управления – относятся к потокам управления, которые намеренно добавляются в программу, но никогда не будут выполнены.

– Числовые схемы – оставляют непрозрачные предикаты с математическими выражениями. Такие непрозрачные предикаты используются для введения поддельных потоков управления.

– Вероятностные потоки управления – похожи на поддельные потоки управления, но отличаются тем, что контекстуальные непрозрачные предикаты вводят мертвые пути, но не вводят ненужные коды.

– Диспетчерское управление – Управление на основе диспетчера определяет следующие блоки кодов, которые будут выполняться во время работы программы. Такие элементы управления необходимы для обфускации потока управления, поскольку они могут скрыть исходные потоки управления от статического анализа программы.

– Неявные элементы управления – явные инструкции управления преобразуются в неявные, это может помешать злоумышленникам адресовать правильные потоки управления.

3. Обфускация данных

– Разделение / объединение данных – распределяет информацию об одной переменной на несколько новых переменных.

– Обработка данных – заменяет статические данные вызовами процедур.

– Кодирование данных – кодирует данные с помощью математических функций или шифров.

– Преобразование массива – применяются методы разделение одного массива на несколько подмассивов, объединение нескольких массивов в один, свертывание массива для увеличения его размерности или выравнивание массива для уменьшения размерности.

4. Обфускация методов

– Встроенный / контурный метод – извлекается последовательность инструкций и абстрагируется метод.

– Клон метода – создаться репликацию метода и вызывается случайным образом.

– Разделение / объединение методов – объединение нерелевантных методов в один или разбиение метода на несколько методов.

5. Обфускация классов

– Удаление модификаторов – снимает ограничения и делает всх члены класса общедоступными.

– Разделение / объединение классов – при объединении классов мы можем передавать локальные переменные или локальные группы инструкций другому классу.

– Изменение иерархии классов – разрыв исходных отношений наследования между классами и интерфейсами, позволяя каждому узлу поддерева в иерархии классов реализовывать один и тот же интерфейс.

В результате исследования методов обфускации были выделены 5 крупных блоков, в зависимости от разницы в их целях обфускации. Каждый уровень дополнительно содержит несколько подкатегорий или стратегий обфускации. При обфускации исходного кода рекомендуется использовать несколько техник запутывания сразу.

Список литературы

1. Зайцев Е.С., Сераджи С.И. Исследование существующих систем обфускации с целью защиты программных алгоритмов/ телекоммуникации и информационные технологии 2019, т. 6, ст. 83-88

2. Abrath, B, Coppens B, Volckaert S, De Sutter B (2015) Obfuscating windows dlls In: 2015 IEEE/ACM 1st International Workshop on Software Protection, 24–30. IEEE. https://doi.org/10.1109/spro.2015.13.

3. Balakrishnan, A, Schulze C (2005) Code obfuscation literature survey. CS701 Constr Compilers.

СТАТИСТИЧЕСКИЙ АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЗА 2020 И 2021 ГОДЫ

Цымбаленко Сергей Михайлович
Студент кафедры Информационной безопасности
Волгоградский государственный университет
qjack228@mail.ru
Проспект Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Проанализированы тренды и общая статистика угрозы в сфере информационной безопасности за 2020 и 2021 года. А также, выявлены приоритеты злоумышленников, определен наиболее распространенный вектор атаки на защищаемые объекты и частные лица.

Ключевые слова: кибератаки, уязвимости, киберинциденты, вредоносное ПО, источники угроз, злоумышленник, безопасность.

STATISTICAL ANALYSIS OF INFORMATION SECURITY THREATS FOR 2020 AND 2021

Tsymbalenko Sergey Mikhailovich
Student of Department of Information Security,
Volgograd State University
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation

Abstract. The trends and general statistics of the threat in the field of information security for 2020 and 2021 are analyzed. And also, the priorities of intruders were identified, the most common attack vector on protected objects and individuals was determined.

Key words: cyber-attacks, vulnerabilities, cyber incidents, malware, threat sources, intruder, security.

В настоящее время, количество кибератак увеличивается практически пропорционально скорости развитию технологий. Такие IT гиганты как Google, Microsoft и Amazon, развивают свою структуру безопасности

быстрее, чем появляются новые специалисты в этой сфере, которые могли бы как-то навредить им. Благодаря большему количеству источников информации для обучения в сфере информационной безопасности, специалистов становится куда больше с каждым годом. Несмотря на быстрое развитие безопасности IT гигантов, количество уязвимых компаний не стало меньше. Ведь компаний, что готовы платить цены за предоставляемые услуги этих самых гигантов, меньшинство. Люди что обучаются этому, изначально нацелены на IT гигантов. Таким образом, безопасность менее крупных компаний, кажется для них не столь большим препятствием. Для предотвращения актуальных угроз, нужно иметь понимание векторов атак. А также иметь актуальный список трендов, дабы избежать большинство вреда со стороны кибератак. Дальнейший анализ статистики покажет масштаб и тренды нынешних угроз в IT сфере.

Данный график показывает, насколько пандемия повлияло на количество кибератак. Самый большой прирост в 59% был в октябре 2020 года, в сравнении с октябрем 2019 года. Львиная доля этих атак была на организации, такие как, промышленные компании, а также государственные и медицинские учреждения.

Пандемия очень сильно повлияла на индустрию. Большинство работников IT перешло на дистанционную работу. Многие учебные учреждения перешли на систему дистанционного обучения. Все это сказалось большой нагрузкой на сервисах, существующих до самой пандемии. Людям нужно было средство связи между собой, из-за чего большинство IT компаний начали в спешке разрабатывать такой сервис. Не обошлось и без уязвимостей в связи с этой спешкой. Много работников использовало ПО для дистанционной работы, такое как VPN, MS Office и прочее. Однако быстро нашлись уязвимости, такие как CVE-2017-11882 и CVE-2019-11510, благодаря которым компании и были подвержены атаке.

Еще одним последствием дистанционной системы, стал большой приток людей в IT сферу. Люди начали находить общедоступные источники

информации для дальнейшего обучения, а также многих привлекла идея смены профессии. Пандемия показала, насколько IT сфера перспективна, что и побудило людей развиваться в этом направлении.

Следующий график (рисунок 1) показывает, что количество кибератак только начало возрастать. В сравнении первых кварталов 2020 и 2021 годов, наблюдается прирост количества атак. Учитывая тренды наплыва новых специалистов и развития безопасности IT компаний, стоит ожидать что количество атак не станет убывать.

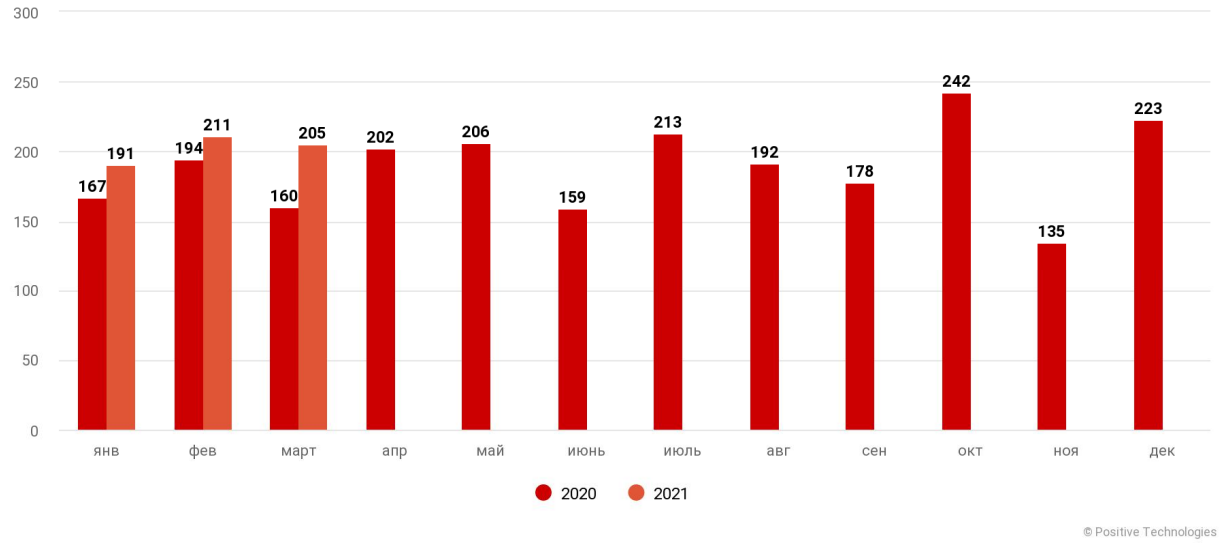

Рис. 1. Количество кибератак по 2020 и 2021 годам

Большинство атак, а именно 77% за 2020 год, были целенаправленными (рисунок 2). Самое большое количество украденных данных пришлось на персональные данные, что составляет 31% от всех других типов. Следующим типом является коммерческая тайна, что составляет 24% от других типов. Отсюда можно понять, что приоритетом безопасности должны быть именно эти структуры, что хранят персональные данные или имеют какое-то отношение к коммерческим тайнам. Любое хранилище данных будет высоким приоритетом для большинства кибератак. Полученные данные могут использоваться для шантажа/выкупа, или-же для продажи на даркнете.

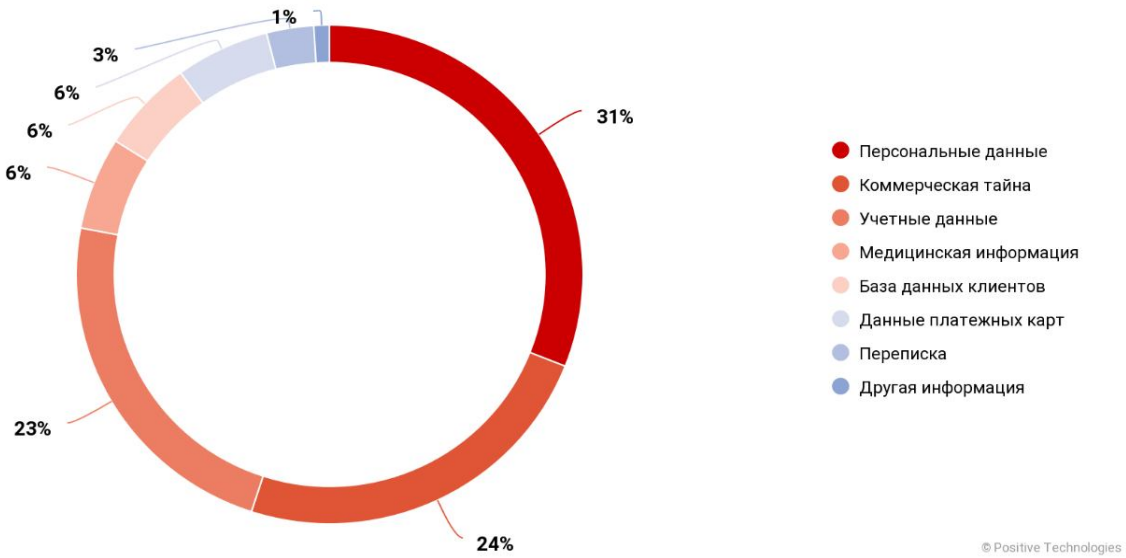

Рис. 2. Типы атак за 2020 год

Основными векторами атаки на частные лица и организации (рисунок 3) является использование ВПО и социальная инженерия. ВПО использовалось в 58% доли атак, следующим идет социальная инженерия, чья доля не сильно уступает доле ВПО.

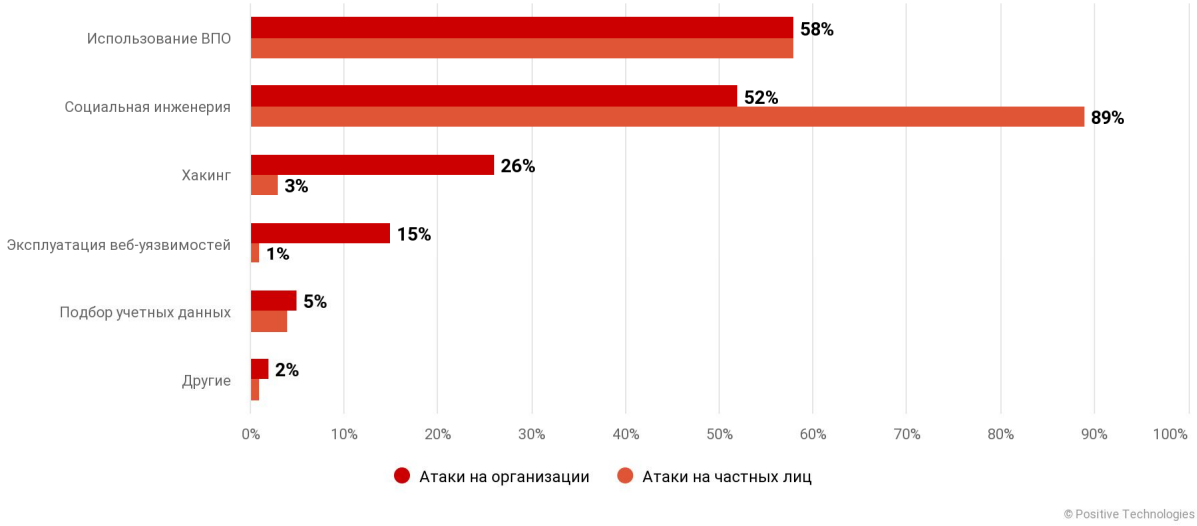

Рис. 3. Векторы атак на частные лица и организации

Самым популярным вредоносным ПО на данный момент, использованным при атаках на организации, является программа-вымогатель. Злоумышленники используют это ПО для шифрования данных самой организации, что в свою очередь может принести большой вред и убытки.

Используя это ПО, злоумышленники требуют выкуп, в обмен на восстановление данных, или-же для предотвращения их распространения по сети. В своем роде это схоже со шпионским ПО, что часто используется для выявления компромата для потенциального вымогания.

Следующее ПО стало самым популярным на момент первого квартала 2021 года:

- REvil
- Clop
- Conti
- Babuk Locker
- DoppelPaymer

В первом квартале 2021 года, создатели REvil (программы-вымогателя), побили рекорд в запрашиваемой сумме выкупа. После успешной атаки на компанию Acer, они потребовали выкуп в размере 50 млн долларов. Также, после успешной атаки на DairyFarm Group, они требовали 30 млн долларов за дешифрование и нераспространение данных. С каждым годом, сумма выкупа растет. Самая ценная часть компании для злоумышленников, это данные. Не создав безопасную структуру для хранения данных, компания подвергает себя возможному взлому, что приводит к большим убыткам и подрыву репутации. В среднем, после успешной атаки на компанию что предоставляет публичный сервис, около 9% пользователей прекращают использование сервиса, перестав доверять свою информационную безопасность этой компании.

Самым часто используемым способом распространения вредоносного ПО на нынешний момент, является электронная почта (рисунок 4). Доля которого составляет 61%. Злоумышленники стремятся занести ПО тем способом, что имеет наименьшее количество проверок при загрузке и отправке. А человеческий фактор, простое незнание о потенциальном вреде что может нести файл, играет на руку злоумышленникам. Однако некоторые компании борются с этим, запретив своим сотрудникам открывать файлы с

электронного письма, или-же вовсе перейдя на другую систему пересылки сообщений, где файлы обрабатываются при загрузке, со стороны отправителя и получателя.

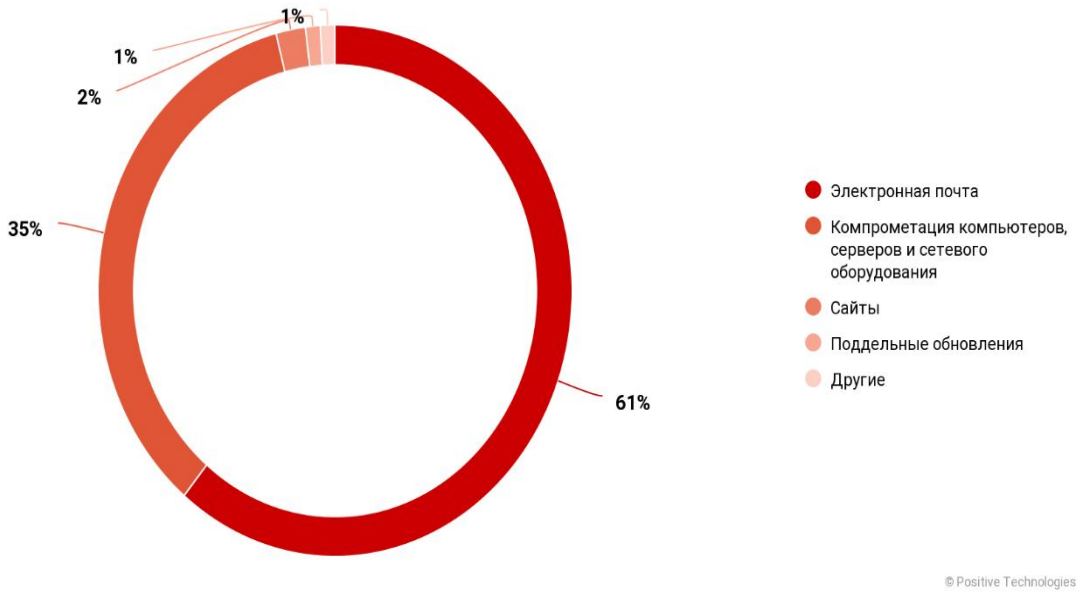

Рис. 4. Способы распространения вредоносного ПО

Благодаря таким системам как Bug Bounty, более простые векторы атак, уже теряют актуальность. Специалистам платят за находку бреши в безопасности сервера и приложений. Однако в молодых, малоразвитых компаниях, такие банальные вещи как DDoS, default credentials и многое другое, может не учитываться. Таких компаний не мало, даже относительно крупные компании допускают очевидные ошибки. Поэтому немаловажно анализировать свою систему безопасности, следить за актуальными трендами и периодически проверять, есть ли пораженные системы или файлы.

Список литературы

1. Актуальные киберугрозы 2020 года – Электрон. текстовые дан. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/

2. Cybersecurity Statistics and Trends for 2021 / Статистика и тенденции кибербезопасности на 2021 год года– Электрон. текстовые дан. – Режим доступа: https://www.varonis.com/blog/cybersecurity-statistics/

3.Актуальные киберугрозы: I квартал 2021 года– Электрон. текстовые дан. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q1/

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ В МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Чумбуридзе Яна Алексеевна
студент Волгоградского государственного университета
yanachumb@gmail.com
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация
Бондарь Юлия Андреевна
Ассистент кафедры информационной безопасности,
Волгоградский государственный университет
julie.bondar@gmail.com
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В статье исследуется проблема безопасности и целостности данных в условиях цифровой трансформации в сфере здравоохранения, рассматривается общая архитектура единой государственной информационной системы в сфере здравоохранения. Обсуждается применение технологий распределенного реестра и блокчейн в сфере здравоохранения.

Ключевые слова: цифровая трансформация, медицинская информационная система, безопасность данных, целостность данных, технологии распределенного реестра, блокчейн.

PROBLEMS OF DATA SECURITY IN HOSPITAL INFORMATION SYSTEM

Chumburidze Yana Alekseevna
student of Volgograd State University
yanachumb@gmail.com
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation

Bondar Yulia Andreevna
assistant of the Department of Information Security of
Volgograd state University
julie.bondar@gmail.com
Prospekt Universitetskij, 100, 400062 Volgograd, Russian Federation

Abstract. This article studies the problem of data security and integrity in the context of digital transformation in the healthcare sector, examines the general architecture of the unified state information system in the healthcare sector. The application of distributed ledger technologyand blockchain technologies in the healthcare sector is discussed.

Key words: digital transformation, hospital information system, data security, data integrity, distributed ledger technology, blockchain.

Цифровая трансформация в сфере здравоохранения является одним из приоритетных направлений развития Российской Федерации[1]. Цифровая трансформация – это процесс перехода рассматриваемой сложной системы из одного состояния в другое под влиянием развития новых информационных технологий. Цифровизация в сфере здравоохранения не только повышает эффективность оказания медицинских услуг, но и увеличивает риски информационной безопасности. На сегодняшний день в качестве результата цифровой трансформации сферы здравоохранения, проводившейся на протяжении последних лет, на федеральном и региональном уровне создана единая государственная информационная система в сфере здравоохранения (ЕГИСЗ).

Рассмотрим общую архитектуру ЕГИСЗ (рисунок 1).

Общая архитектура ЕГИСЗ состоит из трех уровней: федерального, регионального и уровня медицинских информационных систем (МИС).

На первом уровне располагается федеральный центр обработки данных (ЦОД) и подсистемы ЕГИСЗ. На втором уровне размещены ГИС субъектов Российской Федерации в сфере здравоохранения. На третьем уровне

располагаются МИС медицинских организаций (МО), в их состав входят АРМ медицинских сотрудников.

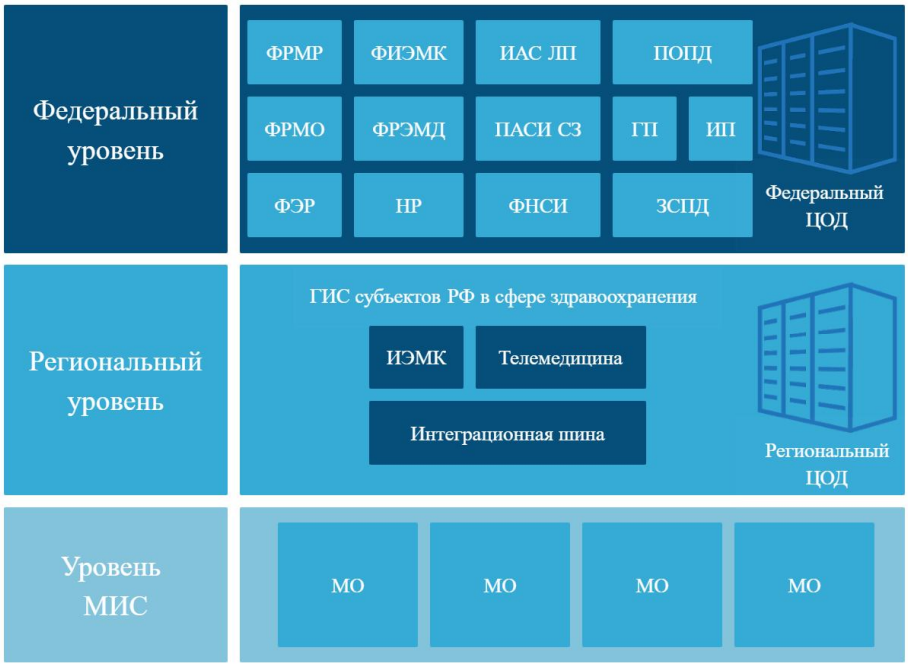

Рис. 1. Общая архитектура ЕГИСЗ

Проблема обеспечения безопасности и целостности медицинских данных при их обработке, хранении и передаче в ЕГИСЗ остается актуальной, поскольку медицинские записи хранятся на уровне МИС МО разрозненно: каждая МО имеет свою базу данных. В некоторых случаях медицинские сведения все еще хранятся на бумажных носителях в единственном экземпляре. Наилучшим образом помогает преодолеть проблемы обеспечения безопасности данных в сфере здравоохранения технология распределенного реестра.

Наиболее распространенной реализацией технологий распределенного реестра является блокчейн. Он основан на принципах криптографии, децентрализации и консенсуса, которые обеспечивают доверие к транзакциям. В блокчейн данные структурированы в блоки, и каждый блок содержит одну или несколько транзакций. Каждый новый блок присоединяется ко всем предшествующим блокам в криптографической цепочке таким образом, что вмешательство невозможно. Все транзакции

внутри блоков проверяются и согласовываются с помощью механизма консенсуса, гарантирующего, что каждая транзакция является правильной.

Применение технологии блокчейн в сфере здравоохранения обеспечит безопасность и целостность медицинских записей пациентов и упростит взаимодействие врачей и пациентов (рисунок 2).

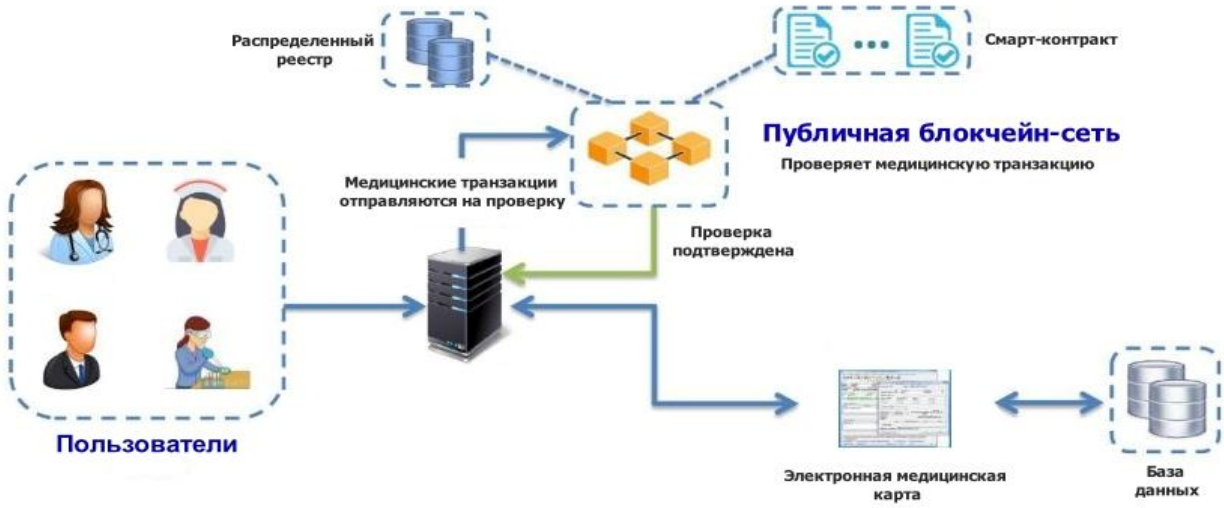

Рис. 2. Применение технологии блокчейн в сфере здравоохранения

Рассмотрим процесс совместного использования электронной медицинской карты на основе блокчейна:

1. Мобильный шлюз инициализирует запрос как новую транзакцию для загрузки данных на облачный сервер.

2. Блокчейн-клиент обрабатывает и отправляет запрос менеджеру и смарт-контрактам для проверки.

3. Менеджер электронной медицинской карточки проверяет запрос с помощью смарт-контрактов с помощью политики строгого контроля. Если запрос принят, ответ будет возвращен шлюзу для загрузки данных.

4. Шлюз теперь может использовать электронную медицинскую карту, т. е. файл данных о состоянии здоровья и шифровать данные с помощью открытого ключа менеджера электронной медицинской карты. Затем мобильный шлюз загружает этот зашифрованный файл в хранилище IPFS в облаке.

5. Хранилище IPFS сохранит файл данных в соответствующем узле хранения, используя информацию о загрузке (идентификатор области, идентификатор пациента), и автоматически вернет значение хэша, которое хранится в таблице DHT.

6. Транзакции загрузки группируются в блоки данных, которые затем вставляются в пул транзакций для подтверждения майнерами для добавления в блокчейн.

7. Транзакция загрузки обновляется на мобильном шлюзе для отслеживания.

8. Пользователь подключается к сети блокчейн, подготавливает транзакцию с информацией о запросе (идентификаторы запроса), и подписывает его закрытым ключом для доступа к данным в облаке.

9. Пользователь подключается к облаку и отправляет запрос на доступ к данным в облако с помощью клиентского модуля блокчейн.

10. Менеджер электронной медицинской карты проверит право доступа пользователя с помощью стратегии контроля доступа с помощью смарт-контракта. Как только запрос на доступ будет подтвержден, менеджер электронной медицинской карты проанализирует запросы и перенаправит информацию в хранилище IPFS для извлечения данных.

11. Менеджер электронной медицинской карты расшифровывает такие запрошенные данные с помощью алгоритма асимметричного шифрования и возвращает эти запрошенные данные запрашивающему лицу.

12. Транзакция загрузки обновляется на мобильном устройстве пользователя для отслеживания через блокчейн-клиент.

Технология блокчейн может преобразовать ИТ-инфраструктуру отрасли здравоохранения из централизованных, изолированных систем в распределенные, децентрализованные системы, что может обеспечить безопасность и целостность медицинских данных, а также значительно улучшить качество оказываемой медицинской помощи.

Список литературы

1. Указ Президента Российской Федерации от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года».

2. Постановление Правительства Российской Федерации от 05.05.2018 № 555 «О единой государственной информационной системе в сфере здравоохранения».

ПРОСВЕТИТЕЛЬСКАЯ РАБОТА ПО ПОВЫШЕНИЮ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ

Яриков Владислав Георгиевич

доцент кафедры методики преподавания математики и физики, ИКТ, канд. пед. наук,

Волгоградский государственный социально-педагогический университет

Аннотация. Выделяются задачи информационной безопасности в системе образования. Производится анализ влияния технологии просветительских мер на обеспечение информационной безопасности.

Ключевые слова: информационные технологии, вопросы информационной безопасности, угрозы информационной безопасности, просветительские меры.

EDUCATIONAL WORK TO INCREASE THE LEVEL OF INFORMATION SECURITY IN EDUCATIONAL INSTITUTIONS

Yarikov Vladislav Georgievich

Associate Professor, Department of Methods of Teaching Mathematics and Physics, ICT Ph.D. ped. Sciences,

Volgograd State Social and Pedagogical University

Abstract. The tasks of information security in the education system are highlighted. An analysis is made of the impact of the technology of educational measures on ensuring information security.

Key words: information technologies, information security issues, information security threats, educational measures.

Актуальность вопроса обусловлена значительными изменениями в социальной, политической и экономической жизни современного общества под влиянием процесса массового использования информационных технологий и активным внедрением дистанционных технологий обучения в систему образования.

Большое значение имеют перемены, спровоцированные масштабным внедрением информационных технологий в сферу образования. Образовательные учреждения перестают быть местом получения готовых и общепринятых знаний, они становятся местом коммуникаций и информационного обмена обучающихся с окружающим миром и взаимодействия с информационными системами, обеспечивающими образовательный процесс. В связи с этим одной из основных задач образования становится задача информационной безопасности обучающихся в образовательных учреждениях всех уровней.

Важным требованием обеспечения деятельности образовательного учреждения на сегодняшний день является поддержание высокого уровня информационной безопасности. Причем вопросы информационной безопасности (ИБ) в образовательных организациях имеют свою специфику. Информационная безопасность в системе образования в целом и в каждом конкретном образовательном учреждении должна представлять собой системный комплекс мероприятий, направленных на реализацию двух основных задач. Помимо защиты информационной системы учреждения, баз данных, как внутренних, так и внешних, и предотвращения хакерских атак, также важно оградить обучающихся от любых проявлений незаконной пропаганды и попыток манипулирования.

Современные технологии в области информационной безопасности, доступные образовательным организациям, которые прописаны в том числе

и на законодательном уровне, предусматривают организацию защиты по следующим направлениям:

- нормативно-правовое;
- морально-этическое;
- административно-организационное;
- техническое;
- просветительское.

Рассмотрим подробнее одно из них, а именно просветительские меры.

Большое значение в области обеспечения информационной безопасности имеют просветительские, иначе их можно назвать профилактические, меры. Постоянная разъяснительная работа среди сотрудников и обучающихся о необходимости защиты информации, персональных данных позволит повысить уровень культуры информационной безопасности и воспринимать задачи информационной безопасности не как помеху в работе, а как важный элемент своей работы и повседневной жизни.

Отдельно необходимо отметить работу, направленную на предотвращение небезопасного использования сетевых ресурсов в целом и социальных сетей в частности. Активность обучающихся и преподавателей в социальных сетях часто приводит к негативным последствиям, связанным с использованием персональных данных злоумышленниками, причем эти данные пользователи нередко размещали в социальных сетях сами.

К числу просветительских мер относятся:

- регулярная просветительная работа;
- проведение обучающих семинаров;
- прохождение сотрудниками профильных курсов повышения квалификации.

Плановое проведение подобных мероприятий позволит не только повысить уровень информационной безопасности образовательного

учреждения, но и уровень личной информационной безопасности сотрудников и обучающихся, их позитивное личностное развитие.

Анализ существующих угроз в сфере информационной безопасности и опасностей использования интернет-ресурсов, в особенности социальных сетей, показал, что деятельность в области информационной безопасности является одним из приоритетных условий развития сферы образования в ближайшем будущем.

Исследования в области культуры ИБ открывает перспективу для дальнейшего изучения проблемы обеспечения информационной безопасности в образовательных учреждениях в контексте культуры безопасности человека XXI века, идей открытого образования и методик информатизации образования.

Список литературы

1. Блог / Информационная безопасность в образовательной организации / Smart-SoftTeam / https://www.smart-soft.ru/blog/informatsionnaja_bezopasnost_v_obrazovateljnoj_organizatsii/ (дата просмотра 01.11.2021)

2. Указ Президента РФ от 1 июня 2012 г. № 761 «О Национальной стратегии действий в интересах детей на 2012–2017 годы» https://base.garant.ru/70183566/#block_1000

3. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (последняя редакция) http://www.consultant.ru/document/cons_doc_LAW_61801/

4. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция) http://www.consultant.ru/document/cons_doc_LAW_61798/

СОДЕРЖАНИЕ

Для заметок

Научное издание

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

МАТЕРИАЛЫ
IX Всероссийской научно-практической конференции
с международным участием

г. Волгоград, 27–28 октября 2021 г.

Главный редактор *Н.В. Горева*
Оформление обложки *Н.Н. Захаровой*

Печатается в авторской редакции с готового оригинал-макета.

Подписано в печать 24.12 2021 г. Формат 60x84/16
Бумага офсетная. Гарнитура Таймс. Усл.-печ. л. 6,1.
Уч.-изд. л. 6,5. Тираж 35 экз. Заказ . «С» 123.

Волгоградский государственный университет.
400062 Волгоград, просп. Университетский, 100.
www.volsu.ru

Отпечатано в издательстве
Волгоградского государственного университета.
400062 Волгоград, ул. Богданова, 32.
E-mail: izvolgu@volsu.ru