УДК 004.056.5

СИСТЕМА КИБЕРБЕЗОПАСНОСТИ СОВРЕМЕННОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

Алекперов И.Д.
к.т.н., доцент
ЧОУ ВО «Южный университет (ИУБиП)»
e–mail: ilgar@iubip.ru
Алекперова Э.А.
преподаватель
ЧОУ ВО «Южный университет (ИУБиП)»
e–mail: emma.alekperova@yandex.ru
Алекперова А.И.
преподаватель
ЧОУ ВО «Южный университет (ИУБиП)»
e–mail: aida2710@yandex.ru
Храмов В.В.
студент ФГБОУ ВО Донской государственный технический (ДГТУ)
e-mail: vvx2002@inbox.ru

Аннотация: Информационные атаки, представляющие собой поэтапную публикацию фейковых новостей в соцсетях и кибератаки. Эпоха цифровизации и процессы цифровой трансформации грозят снова изменить парадигму защиты – все становится цифровым и вместе с возможностями порождает и новые риски. Методики систем защиты в области кибербезопасности образовательного учреждения и предложены конкретные инструменты по их внедрению.
Ключевые слова: информатизация, система защиты, образовательная система, информация, цифровизация, цифровая грамотность, кибербезопасность, защита информации.

CYBERSECURITY SYSTEM OF A MODERN EDUCATIONAL INSTITUTION

Alekperov I.D.
Alekperova E.A.

Alekperova A.I.
Khramov V.V.

Abstract: Information attacks, which are the gradual publication of fake news in social networks and cyber attacks. The era of digitalization and the processes of digital transformation threaten to change the paradigm of protection again – everything becomes digital and together with opportunities creates new risks. Methods of protection systems in the field of cybersecurity of educational institutions and specific tools for their implementation are proposed.
Keywords: Informatization, security system, educational system, information, digitalization, digital literacy, cybersecurity, information protection.

За последний десяток лет отрасль информационной безопасности претерпела те же изменения, что и сфера информационных технологий десятью годами раньше. Однако за последнее десятилетие началась необратимая сегментация и информационной безопасности. Необратимая потому, что, специализируясь в чем-то одном, сотрудник начинал отставать в других областях, которые тем временем развивались семимильными шагами, и догнать их становилось все труднее с каждым днем [1].

За минувшее время сам объект защиты, информационная система и хранящиеся в ней сведения тоже переродились и продолжают меняться сегодня. Атаки «шифровальщиков» последних лет показали, что даже если организация имеет традиционный, абсолютно стандартную систему образования, в любом случае осуществлять деятельность без системы информационной безопасности невозможно [2].

Информационные атаки, представляющие собой поэтапную публикацию фейковых новостей в соцсетях и кибератаки. То есть, например, массовые публикации о том, что у какого-то образовательного учреждения вот-вот отберут лицензию, сочетаются с атакой на цифровые сервисы этой организации. Заказчики услуг читают публикации, идут проверять сайт образовательного учреждения – сервисы недоступны [3]. Клиенты нервничают и торопятся в образовательное учреждение, где встречают сотни таких же взволнованных людей. Они возмущенно пишут об этом в соцсетях, что вызывает только новый приток обеспокоенных заказчиков. Организаторы

атаки уже могут уходить, поскольку запущенный ими процесс стал самоподдерживающимся [4].

Эпоха цифровизации и процессы цифровой трансформации грозят снова изменить парадигму защиты – все становится цифровым и вместе с возможностями порождает и новые риски. Угроз ИТ-системам стало много, а средств противодействия им – еще больше. И информационная безопасность постоянно сегментируется. Сегодня невозможно одинаково хорошо разбираться в антивирусах, брандмауэрах, системах аутентификации доступа и физической безопасности [5]. И это лишь защита, а есть же еще offensive security и связанные с ней тесты на проникновение, исследование защищенности систем и т.п. А еще облака, нейросетки, блокчейн, искусственный интеллект и «машин-лернинг»... Есть мониторинг соцсетей для предотвращения информационных атак. Есть внутренний контроль и работа с кадрами. И, конечно, бумажная безопасность – соответствие требованиям многочисленных международных, государственных и отраслевых регуляторов [6].

Оказалось, что подготовка миллиона программистов для цифровой экономики – на порядок более простая задача, чем подготовка даже десяти тысяч специалистов в области цифрой безопасности - стражей цифровой экономики.

Цифровизация предполагает постоянные изменения автоматизированных процессов, быструю их адаптацию под требования бизнеса. Поэтому безопасность, как свойство процесса, должна перестраиваться не после, как сегодня, а во время изменений. Сегодняшний процесс обеспечения безопасности, в котором сначала создается объект защиты, потом его защищенность тестируют, возвращают разработчикам замечания, те их исправляют, объект снова тестируется и т.п., уже не удовлетворяет требованиям по скорости изменений [7].

Это может поменять сам смысл определения «информационная безопасность» или придать новый смысл безопасности «цифровой»,

сочетающей элементы кибербезопасности, безопасности цифровых активов (репутации, бренда), бизнес-эффективности и офлайновой, материальной, безопасности. Таким образом, в цифровом мире роль безопасности может раствориться в смежных дисциплинах: ИТ, разработке, поддержке, кадровой безопасности, внутреннем контроле, даже PR и маркетинге (информационные атаки через социальные сети отражать придется вместе с ними). Возможно, квалификация в области безопасности станет обязательным требованием для некоторых специальностей, а не отдельной профессией [8].

По результатам проведенных исследований основных мер по обеспечению кибербезопасности в цифровой среде в рамках сотрудничества между Министерством общего и профессионального образования Ростовской области и Частным образовательным учреждением высшего образования (ЧОУ ВО) «Южным университетом (ИУБиП)» по реализации проекта «Кибербезопасность в эпоху цифрового образования» были разработаны методики систем защиты в области кибербезопасности образовательного учреждения и предложены конкретные инструменты по их внедрению [9].

В первую очередь были определены формы и мотивы киберпреступности. Специалисты выделили четыре основные формы преступного воздействия на киберпространстве:

1. Финансовые махинации.
2. Кража данных учетных записей.
3. Вредоносные программы.
4. Неосторожность пользователя.

Против финансовых махинаций специалистами были предложены следующие способы защиты:

1. Избегать приобретения что-либо в Интернете, используя платные SMS-сообщения.
2. К основной карте, которой расплачиваются в интернете, нужно переводить небольшие суммы денег с дополнительной карты во время

транзакции, а в «случае компрометации данных достаточно просто заблокировать ее.

3. Регулярно проверять состояние банковских счетов, чтобы убедиться в отсутствии «лишних» и странных операций.
4. Хранить номер карточки и ПИН–коды в тайне. Лучше запомнить и стереть (заклеить) CVC-код
5. Использовать виртуальные карты, которые сейчас предоставляют платежные системы.
6. Поставить лимит на сумму списаний или перевода в личном кабинете банка»[4].

Против кражи учетных данных были предложены следующие механизмы защиты:

1. Использовать сложные пароли.
2. Не опубликовать в «социальных сетях данные, попадание которых в свободный доступ недопустимо.
3. Не заполнять полученные по электронной почте формы и анкеты. Личные данные безопасно вводить только на защищенных сайтах.
4. Проверять запросы персональных данных из каких-либо деловых и финансовых структур. Лучше обратиться в эти структуры по контактам, указанным на официальном сайте, а не в электронном письме.
5. Насторожиться, если кроме вас в электронном сообщении указаны другие адресаты. Крайне маловероятно, чтобы при общении с клиентом по поводу личных учетных данных банк ставил кого-то в копию»[4].

Против вредоносных программ были предложены следующие способы защиты:

1. Пользоваться защитным программным обеспечением – антивирус и межсетевой экран (файрвол).

2. Быть «осмотрительным в отношении писем с вложенными картинками, поскольку файлы могут содержать вирусы. Открывать вложения только от известных вам отправителей. И всегда проверять вложения на наличие вирусов, если это возможно.
3. Не переходить необдуманно по ссылкам, содержащимся в письмах и сообщениях. Удостовериться в правильности ссылки, прежде чем переходить по ней из электронного письма»[4].

По борьбе с неосторожность пользователя были предложены следующие способы защиты:

1. Никогда не передавать «конфиденциальные данные в ответ на письма или сообщения в социальных сетях.
2. С осторожностью относится к неправдоподобно выгодным предложениям финансового характера.
3. Пользоваться свежими версиями программного обеспечения. Это касается всего программного обеспечения на компьютере, особенно операционной системы, веб-браузера, защитного ПО»[5].
4. На запрос мошенников с требованием о немедленных действиях, представляя ту или иную ситуацию чрезвычайной, сохранять спокойствие, удостовериться в правильности предоставляемой информации. Преступники вызывают ощущение тревоги, чтобы заставить действовать быстро и неосмотрительно.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Алекперов И.Д. Разработка информационного ресурса выпускников “Школы развития личности и успеха ИУБиП” в интернет пространстве с использованием языков программирования PHP, MySQL. – Ростов-на-Дону: Институт управления, бизнеса и права, 2013.
2. Алекперов И.Д. Электронная коммерция (E–commerce). [Электронный ресурс] LAP LAMBERT Academic Publishing. ISBN 978–3–330–35282–7, URN: 101:1–201708141845, EAN: 9783330352827. – URL: http://d–nb.info/Erschei–nungsdatum: 2017 г. (дата обращения 07.06.2019 г.).
3. Алекперов И.Д. Электронный бизнес–консалтинг как средство развития региональной электронной коммерции // Интеллектуальные ресурсы – региональному развитию. – 2016. – №2. – С. 6-9.

4. Рекомендации безопасного поведения при использовании сети «интернет» и сотовой связи. Киберпреступность [Электронный ресурс] – URL: https://anadir.bezformata.com/listnews/internet-i-sotovoj-svyazi-kiberprestupnost /60940911/
5. Алекперов И.Д. , Храмов В.В., Горбачева А.А., Фомичев Д.П. Информационная безопасность и защита информации в цифровой экономике элементы теории и тестовые задания: учеб. пособие / ЮУ (ИУБиП). – Ростов-на-Дону, 2019. – 114 с.
6. Голубенко Е.В., Ковтун О.Г., Храмов В.В. Информационная безопасность и защита информации на транспорте: Тестовые задания по дисциплине. – Ростов–на–Дону, 2015. [Электронный ресурс]. – URL: https://elibrary.ru/item.asp7idKJ6311930 (дата обращения 12.02.2020 г.).
7. Литвинов С.А., Алекперов И.Д. Проблемные аспекты реализации кибербезопасности в XXI веке // Интеллектуальные ресурсы – региональному развитию». – 2020. – №1.
8. Храмов В.В. Основы методологии синтеза средств защиты информации // Проблемы обеспечения эффективности и устойчивости функционирования сложных технических систем: Материалы XXI Межведомственной научно-технической конференции. –2002.– С. 115–120. – URL: https://elibrary.ru/item.asp7idKJ2877301 (дата обращения 12.02.2020 г.).
9. Губарев О.К.,Храмов В.В. Способ повышения безопасности программных средств и пути его реализации // Тематический научно–технический сборник. – Пущино, Научный Центр РАН, 1994. –С. 56–61. – URL: https://elibrary.ru/item.asp/ (дата обращения 12.12.2019 г.).