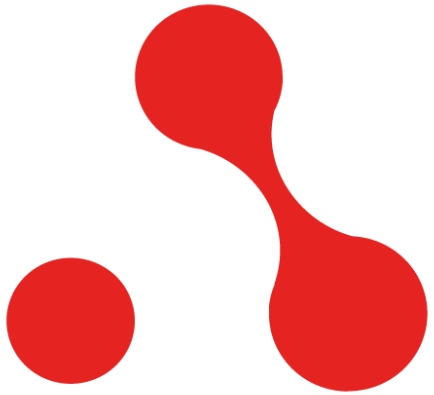

AIC

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ДЛЯ УНИВЕРСИТЕТОВ

IT Teams & Services

СТРУКТУРА УНИВЕРСИТЕТОВ ПОДВЕРЖЕННЫХ КИБЕРАТАКАМ

AIC

Кибератаки могут быть направлены на разные уровни инфраструктуры университета. Рассмотрим основные целевые объекты:

Административные системы

ЦЕЛЬ АТАК:

- Кража персональных данных студентов и сотрудников.
- Манипуляция финансовыми документами.
- Блокировка работы университетских сервисов.

Образовательные платформы (LMS – Learning Management System)

ЦЕЛЬ АТАК:

- Изменение оценок студентов.
- Кража учебных материалов и экзаменационных заданий.
- Саботаж образовательного процесса.

Исследовательские центры и лаборатории

ЦЕЛЬ АТАК:

- Кража научных данных и патентов.
- Саботаж исследований.
- Интеллектуальный шпионаж.

:

Университетские сети и Wi-Fi

ЦЕЛЬ АТАК:

- Перехват трафика студентов и сотрудников.
- Организация MITM-атак (Man-in-the-Middle).
- Распространение вредоносного ПО через университетскую сеть.

Медицинские и биотехнологические факультеты

ЦЕЛЬ АТАК:

- Кража медицинских данных пациентов (если есть клиники при вузе).
- Шпионаж в биотехнологиях.
- Вредоносное вмешательство в медицинские системы.

Университетские библиотеки и архивы

ЦЕЛЬ АТАК:

- Удаление или манипуляция академическими ресурсами.
- Кража редких или конфиденциальных документов.

Университетские СМИ и онлайн-порталы

ЦЕЛЬ АТАК:

- Распространение дезинформации.
- Взлом официального сайта университета.
- Саботаж новостных порталов.

ВЫВОД

Киберугрозы могут затронуть любую часть университетской инфраструктуры.

ОСНОВНЫЕ ЦЕЛИ АТАК:

- Персональные данные
- Финансовые ресурсы
- Научные исследования
- Образовательный процесс.

ТИПЫ КИБЕРАТАК НА УНИВЕРСИТЕТЫ

AIC

ВИД КИБЕРАТАКИ	ЦЕЛЬ	МЕТОДЫ	РИСКИ	
Фишинг и социальная инженерия	Кража учетных данных сотрудников и студентов.	\Поддельные письма от администрации университета с просьбой ввести логин и пароль. \Фейковые сайты университетов для сбора данных.	Кража учетных данных Компрометация корпоративных систем Финансовые потери Утечка конфиденциальной информации	Распространение вредоносного ПО Репутационные потери Эксплуатация доверия
Атаки на веб-сайты и системы управления обучением (LMS)	Нарушение работы образовательных платформ (Moodle, Canvas и др.).	\SQL-инъекции (внедрение вредоносных SQL-запросов). \XSS-атаки (использование вредоносного JavaScript-кода). \Подмена оценок и взлом экзаменационных систем.	Кража персональных данных Неавторизованный доступ Финансовые махинации Распространение вредоносного ПО	DDoS-атаки Фальсификация учебных материалов Компрометация исследовательских данных Репутационные потери
Вредоносное ПО (Malware, Ransomware)	Шифрование данных, кража информации.	\Вредоносные файлы в почте (документы, ссылки). \Вирусы, распространяемые через USB-накопители.	Блокировка доступа к данным Кража личной информации Компрометация учетных записей Удаление или изменение данных	Распространение вредоносного ПО Финансовые потери Сбои в работе LMS и IT-инфраструктуры Репутационные риски
DDoS-атаки	Перегрузка серверов, отключение онлайн-систем.	\Массированные запросы к веб-сайтам и онлайн-курсам. \Использование ботнетов для атак.	Нарушение учебного процесса Сбой административных систем Финансовые потери Ухудшение репутации	Сбои в исследовательской деятельности Эксплуатация уязвимостей Шантаж и вымогательство
Взлом Wi-Fi и MITM-атаки (Man-in-the-Middle)	Перехват данных студентов и преподавателей.	\Создание фейковых Wi-Fi точек («университет_WiFi_free»). \Прослушка трафика в университетской сети.	Перехват данных Компрометация учетных записей Подмена трафика Распространение вредоносного ПО	Шпионаж и утечка данных Неавторизованный доступ в сеть Снижение производительности сети Риски для IoT-устройств

ПРИМЕРЫ ВЗЛОМОВ

AIC

УНИВЕРСИТЕТЫ КАЗАХСТАНА, 2019 ГОД

Группа хакеров KazHackMe взломала сайты нескольких казахстанских вузов, включая АУЭС, КарГУ и Казахстанский инженерно-технический университет, продемонстрировав уязвимости в их системах безопасности.

УНИВЕРСИТЕТЫ КОЛОРАДО И МАЙАМИ (США), 2021 ГОД

Операторы шифровальщика Clop атаковали данные двух университетов, используя уязвимости в устаревшем файлообменном решении Accellion FTA. В результате были похищены и опубликованы конфиденциальные данные студентов и сотрудников.

УНИВЕРСИТЕТ БЛЮФИЛД (США), 2021 ГОД

Хакерская группа Avos взломала системы университета и использовала внутреннюю систему оповещения RamAlert для отправки SMS-сообщений всем студентам с уведомлением об атаке. Университет признал взлом и рекомендовал не переходить по ссылкам из этих сообщений.

НЬЮ-ЙОРКСКИЙ УНИВЕРСИТЕТ (США), 2025 ГОД

В результате атаки на сайт университета были раскрыты личные данные более трёх миллионов абитуриентов за последние тридцать лет, включая имена, результаты тестов и другую конфиденциальную информацию.

УНИВЕРСИТЕТ НЬЮКАСЛА (ВЕЛИКОБРИТАНИЯ), 2020 ГОД

Киберпреступники атаковали компьютерную сеть университета, похитили данные и зашифровали исходные файлы с помощью вредоносного ПО Doppel Paymer. Это привело к серьёзным сбоям в работе университета, включая необходимость ручной регистрации студентов.

ЭТИ ИНЦИДЕНТЫ ПОДЧЁРКИВАЮТ НЕОБХОДИМОСТЬ УСИЛЕНИЯ МЕР КИБЕРБЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ ДЛЯ ЗАЩИТЫ ДАННЫХ И ОБЕСПЕЧЕНИЯ СТАБИЛЬНОЙ РАБОТЫ.

РЕШЕНИЕ:
ЗАЩИТА УНИВЕРСИТЕТОВ ОТ КИБЕРАТАК

AIC

ТЕХНИЧЕСКИЕ МЕРЫ ЗАЩИТЫ
БЕЗОПАСНОСТЬ СЕТИ И СЕРВЕРОВ

ЗАЩИТА УНИВЕРСИТЕТСКОЙ СЕТИ:

- Настройка **межсетевых экранов (firewall)** для фильтрации трафика.
- Использование **систем обнаружения и предотвращения вторжений (IDS/IPS)**.

ШИФРОВАНИЕ ДАННЫХ:

- Использование **SSL/TLS** для защиты передаваемых данных.
- **Шифрование баз данных** с конфиденциальной информацией.

БЕЗОПАСНОСТЬ WI-FI:

- Отключение открытых сетей Wi-Fi, внедрение WPA3.
- Использование VPN для удалённого доступа.

АНТИВИРУСНЫЕ РЕШЕНИЯ:

- Установка EDR-систем (Endpoint Detection and Response).
- Регулярное обновление антивирусного ПО.

РЕШЕНИЕ:
ЗАЩИТА УНИВЕРСИТЕТОВ ОТ КИБЕРАТАК

AIC

ЗАЩИТА ПОЛЬЗОВАТЕЛЕЙ И ИХ УЧЕТНЫХ ЗАПИСЕЙ

АУТЕНТИФИКАЦИЯ И УПРАВЛЕНИЕ ДОСТУПОМ

- Обязательное использование **двухфакторной аутентификации (2FA).**
- Разграничение прав доступа: минимально необходимый доступ для каждого сотрудника.
- Регулярная проверка учетных записей (удаление неактивных пользователей).

ЗАЩИТА ОТ ФИШИНГА И АТАК СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

- Фильтрация фишинговых писем в почтовых сервисах.
- Обучение персонала и студентов по кибергигиене.
- Симуляция фишинговых атак для тренировки сотрудников.

ЗАЩИТА ОБРАЗОВАТЕЛЬНЫХ ПЛАТФОРМ И ВЕБ-РЕСУРСОВ

- Регулярное обновление LMS (Moodle, Canvas и др.) и других образовательных платформ.
- Проведение тестирования на уязвимости (Pentest).
- Ограничение API-доступа к университетским базам данных.
- Настройка WAF (Web Application Firewall) для защиты сайтов.

О НАС

AIC

5
Команд

20 лет
На рынке

25+
Специалистов

10 лет
IT support

500+
Реализованных проектов

НАШИ ВЕНДОРА

AIC

2013
Cisco Premier Partner
2017
Партнёрство Splunk, Fortinet и другие вендоры

2019
Первый Gold Partner Fortinet в Центральной Азии
2019
Splunk №1 по компетенции в Центральной Азии

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

AIC

NGFW
CheckPoint, Forcepoint, Fortinet, CISCO, Palo Alto

SIEM
Splunk, Qradar, Logrythm, Energy Logserver, Cortex, Xsiam

DLP
Forcepoint, GTB, Ibatyr, Staffcop, Solar Dozor

EDR/XDR
TrendMicro, CrowdStrike, Fidelis, Cortex XDR

MDM
Citrix, Checkpoint

Sandbox
CheckPoint, Forcepoint, Fortinet, Palo Alto

WAF
Fortinet, F5

PAM
Cyber Ark, Fudo, Wallix

Vulnerability Management
Tenable, Rapid 7, Qualys

Vulnerability Scanner
DerScanner, Nessys

Automated Security Awareness Platform

СЕТЕВАЯ ИНФРАСТРУКТУРА

AIC

Более 20 лет в построении сетей и в сетевой безопасности

ДОСТИЖЕНИЯ

AIC

Внедрили самую крупную Mobile Device Management систему в Казахстане, что позволило банку защитить компанию от убытков на сумму более 22 млрд. тенге.

Реализовали проект (КиберЩит) по защите и разделению промышленных и пользовательских сетей для лидера в электроэнергетической отрасли РК (9 крупных станций).

Провели слияния сетевых инфраструктур двух банков в единую сеть.

Организовали сеть SD-WAN для 98 филиалов крупного строительного холдинга.

Модернизировали центральную сеть передачи данных провайдера и создали новую топологию (кольцо).

Внедрение и поддержка контакт-центров для финансовой отрасли.


Eurasian Bank
HALYK BANK
Altyn Bank
Дочерний Банк China CITIC Bank Corporation Limited
НАЦИОНАЛЬНЫЙ БАНК КАЗАХСТАНА
BI GROUP
ОТБАСЫ БАНК
KPMG
HOME CREDIT BANK
СБЕРБАНК
air astana
TELE2
AIC
НАМ ДОВЕРЯЮТ
KAZZINC
EY
BAITEREK
ХАМЛЕ
Nazarbayev Intellectual Schools
NIS
Kcell
ROYAL PETROL
ForteBank
Bereke Bank
Kaspi.kz
مصرف الهلال
ahilabank
RG BRANDS
FOR A LIFE
SHINHAN BANK KAZAKHSTAN
KEGOC
bcckz
Beeline
NARXOZ
UNIVERSITY
JUSAN

AIC

DEVELOPER AND INTEGRATOR

КАЗАХСТАН г. Алматы
Проспект Аль-Фараби, БЦ Нурлы-Тау 17/1
к5Б +7 771 070 75 85

sales@aic.kz www.aic.kz office@aic.kz